



Network Address Translation (NAT) for Firepower Threat Defense

The following topics explain Network Address Translation (NAT) and how to configure it on Firepower Threat Defense devices.

- [Why Use NAT?, on page 1](#)
- [NAT Basics, on page 2](#)
- [Guidelines for NAT, on page 10](#)
- [Configure NAT for Threat Defense, on page 14](#)
- [Examples for NAT, on page 44](#)
- [History for FTD NAT, on page 63](#)

Why Use NAT?

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private, not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of NAT is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security—Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions—Overlapping IP addresses are not a problem when you use NAT.

- Flexibility—You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.
- Translating between IPv4 and IPv6 (Routed mode only) —If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.



Note NAT is not required. If you do not configure NAT for a given set of traffic, that traffic will not be translated, but will have all of the security policies applied as normal.

NAT Basics

The following topics explain some of the basics of NAT.

NAT Terminology

This document uses the following terminology:

- Real address/host/network/interface—The real address is the address that is defined on the host, before it is translated. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the inside network would be the “real” network. Note that you can translate any network connected to the device, not just an inside network. Therefore if you configure NAT to translate outside addresses, “real” can refer to the outside network when it accesses the inside network.
- Mapped address/host/network/interface—The mapped address is the address that the real address is translated to. In a typical NAT scenario where you want to translate the inside network when it accesses the outside, the outside network would be the “mapped” network.



Note During address translation, IP addresses configured for the device interfaces are not translated.

- Bidirectional initiation—Static NAT allows connections to be initiated *bidirectionally*, meaning both to the host and from the host.
- Source and destination NAT—For any given packet, both the source and destination IP addresses are compared to the NAT rules, and one or both can be translated/untranslated. For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address.

NAT Types

You can implement NAT using the following methods:

- Dynamic NAT—A group of real IP addresses are mapped to a (usually smaller) group of mapped IP addresses, on a first come, first served basis. Only the real host can initiate traffic. See [Dynamic NAT, on page 15](#).
- Dynamic Port Address Translation (PAT)—A group of real IP addresses are mapped to a single IP address using a unique source port of that IP address. See [Dynamic PAT, on page 20](#).
- Static NAT—A consistent mapping between a real and mapped IP address. Allows bidirectional traffic initiation. See [Static NAT, on page 27](#).
- Identity NAT—A real address is statically translated to itself, essentially bypassing NAT. You might want to configure NAT this way when you want to translate a large group of addresses, but then want to exempt a smaller subset of addresses. See [Identity NAT, on page 35](#).

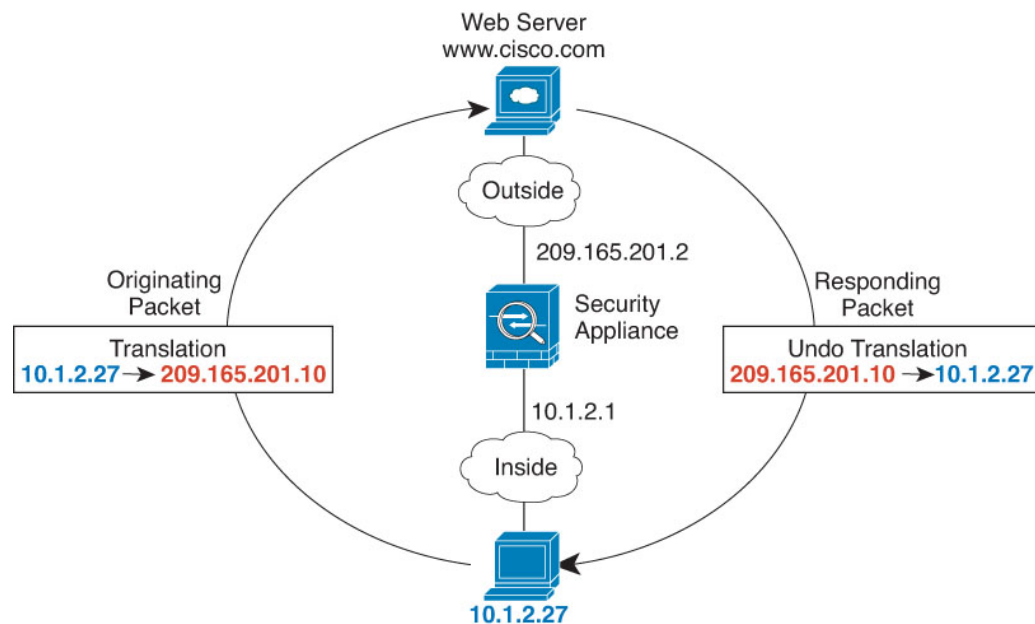
NAT in Routed and Transparent Mode

You can configure NAT in both routed and transparent firewall mode. You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes. The following sections describe typical usage for each firewall mode.

NAT in Routed Mode

The following figure shows a typical NAT example in routed mode, with a private network on the inside.

Figure 1: NAT Example: Routed Mode



1. When the inside host at 10.1.2.27 sends a packet to a web server, the real source address of the packet, 10.1.2.27, is translated to a mapped address, 209.165.201.10.
2. When the server responds, it sends the response to the mapped address, 209.165.201.10, and the FTD device receives the packet because the FTD device performs proxy ARP to claim the packet.

3. The FTD device then changes the translation of the mapped address, 209.165.201.10, back to the real address, 10.1.2.27, before sending it to the host.

NAT in Transparent Mode

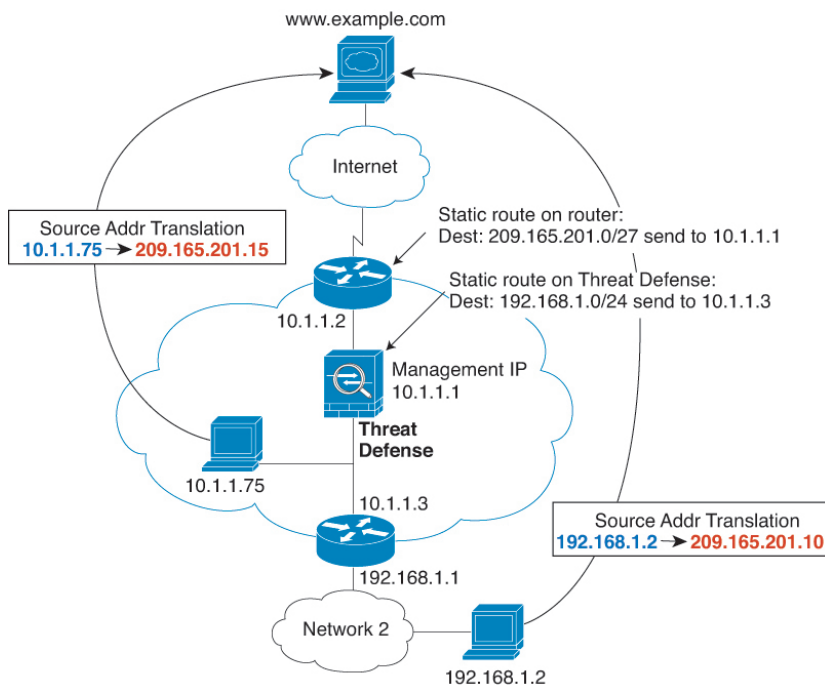
Using NAT in transparent mode eliminates the need for the upstream or downstream routers to perform NAT for their networks.

NAT in transparent mode has the following requirements and limitations:

- You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.
- ARP inspection is not supported. Moreover, if for some reason a host on one side of the FTD sends an ARP request to a host on the other side of the FTD, and the initiating host real address is mapped to a different address on the same subnet, then the real address remains visible in the ARP request.
- Translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.

The following figure shows a typical NAT scenario in transparent mode, with the same network on the inside and outside interfaces. The transparent firewall in this scenario is performing the NAT service so that the upstream router does not have to perform NAT.

Figure 2: NAT Example: Transparent Mode



1. When the inside host at 10.1.1.75 sends a packet to a web server, the real source address of the packet, 10.1.1.75, is changed to a mapped address, 209.165.201.15.
2. When the server responds, it sends the response to the mapped address, 209.165.201.15, and the FTD receives the packet because the upstream router includes this mapped network in a static route directed to the FTD management IP address.

3. The FTD then undoes the translation of the mapped address, 209.165.201.15, back to the real address, 10.1.1.1.75. Because the real address is directly-connected, the FTD sends it directly to the host.
4. For host 192.168.1.2, the same process occurs, except for returning traffic, the FTD looks up the route in its routing table and sends the packet to the downstream router at 10.1.1.3 based on the FTD static route for 192.168.1.0/24.

Auto NAT and Manual NAT

You can implement address translation in two ways: *auto NAT* and *manual NAT*.

We recommend using auto NAT unless you need the extra features that manual NAT provides. It is easier to configure auto NAT, and it might be more reliable for applications such as Voice over IP (VoIP). (For VoIP, you might see a failure in the translation of indirect addresses that do not belong to either of the objects used in the rule.)

Auto NAT

All NAT rules that are configured as a parameter of a network object are considered to be *auto NAT* rules. This is a quick and easy way to configure NAT for a network object. You cannot create these rules for a group object, however.

Although these rules are configured as part of the object itself, you cannot see the NAT configuration in the object definition through the object manager.

When a packet enters an interface, both the source and destination IP addresses are checked against the auto NAT rules. The source and destination address in the packet can be translated by separate rules if separate matches are made. These rules are not tied to each other; different combinations of rules can be used depending on the traffic.

Because the rules are never paired, you cannot specify that sourceA/destinationA should have a different translation than sourceA/destinationB. Use manual NAT for that kind of functionality, where you can identify the source and destination address in a single rule.

Manual NAT

Manual NAT lets you identify both the source and destination address in a single rule. Specifying both the source and destination addresses lets you specify that sourceA/destinationA can have a different translation than sourceA/destinationB.



Note For static NAT, the rule is bidirectional, so be aware that “source” and “destination” are used in commands and descriptions throughout this guide even though a given connection might originate at the “destination” address. For example, if you configure static NAT with port address translation, and specify the source address as a Telnet server, and you want all traffic going to that Telnet server to have the port translated from 2323 to 23, then you must specify the *source* ports to be translated (real: 23, mapped: 2323). You specify the source ports because you specified the Telnet server address as the source address.

The destination address is optional. If you specify the destination address, you can either map it to itself (identity NAT), or you can map it to a different address. The destination mapping is always a static mapping.

Comparing Auto NAT and Manual NAT

The main differences between these two NAT types are:

- How you define the real address.
 - Auto NAT—The NAT rule becomes a parameter for a network object. The network object IP address serves as the original (real) address.
 - Manual NAT—You identify a network object or network object group for both the real and mapped addresses. In this case, NAT is not a parameter of the network object; the network object or group is a parameter of the NAT configuration. The ability to use a network object *group* for the real address means that manual NAT is more scalable.
- How source and destination NAT is implemented.
 - Auto NAT— Each rule can apply to either the source or destination of a packet. So two rules might be used, one for the source IP address, and one for the destination IP address. These two rules cannot be tied together to enforce a specific translation for a source/destination combination.
 - Manual NAT—A single rule translates both the source and destination. A packet matches one rule only, and further rules are not checked. Even if you do not configure the optional destination address, a matching packet still matches one manual NAT rule only. The source and destination are tied together, so you can enforce different translations depending on the source/destination combination. For example, sourceA/destinationA can have a different translation than sourceA/destinationB.
- Order of NAT Rules.
 - Auto NAT—Automatically ordered in the NAT table.
 - Manual NAT—Manually ordered in the NAT table (before or after auto NAT rules).

NAT Rule Order

Auto NAT and manual NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Table 1: NAT Rule Table

Table Section	Rule Type	Order of Rules within the Section
Section 1	Manual NAT	<p>Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, manual NAT rules are added to section 1.</p> <p>By "specific rules first," we mean:</p> <ul style="list-style-type: none"> • Static rules should come before dynamic rules. • Rules that include destination translation should come before rules with source translation only. <p>If you cannot eliminate overlapping rules, where more than one rule might apply based on the source or destination address, be especially careful to follow these recommendations.</p>
Section 2	Auto NAT	<p>If a match in section 1 is not found, section 2 rules are applied in the following order:</p> <ol style="list-style-type: none"> 1. Static rules. 2. Dynamic rules. <p>Within each rule type, the following ordering guidelines are used:</p> <ol style="list-style-type: none"> 1. Quantity of real IP addresses—From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. 2. For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. 3. If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, abracadabra is assessed before catwoman.
Section 3	Manual NAT	<p>If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.</p>

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)

- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object def)
- 172.16.1.0/24 (dynamic) (object abc)

The resultant ordering would be:

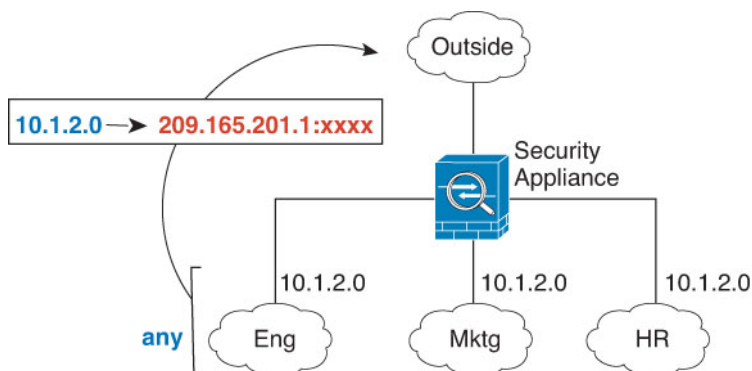
- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object abc)
- 172.16.1.0/24 (dynamic) (object def)
- 192.168.1.0/24 (dynamic)

NAT Interfaces

Except for bridge group member interfaces, you can configure a NAT rule to apply to any interface (in other words, all interfaces), or you can identify specific real and mapped interfaces. You can also specify any interface for the real address, and a specific interface for the mapped address, or vice versa.

For example, you might want to specify any interface for the real address and specify the outside interface for the mapped address if you use the same private addresses on multiple interfaces, and you want to translate them all to the same global pool when accessing the outside.

Figure 3: Specifying Any Interface



Note You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes.

Configuring Routing for NAT

The Firepower Threat Defense device needs to be the destination for any packets sent to the translated (mapped) address.

When sending packets, the device uses the destination interface if you specify one, or a routing table lookup if you do not, to determine the egress interface. For identity NAT, you have the option to use a route lookup even if you specify a destination interface.

The type of routing configuration needed depends on the type of mapped address, as explained in the following topics.

Addresses on the Same Network as the Mapped Interface

If you use addresses on the same network as the destination (mapped) interface, the FTD device uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the FTD device does not have to be the gateway for any additional networks. This solution is ideal if the outside network contains an adequate number of free addresses, a consideration if you are using a 1:1 translation like dynamic NAT or static NAT. Dynamic PAT greatly extends the number of translations you can use with a small number of addresses, so even if the available addresses on the outside network is small, this method can be used. For PAT, you can even use the IP address of the mapped interface.



Note If you configure the mapped interface to be any interface, and you specify a mapped address on the same network as one of the mapped interfaces, then if an ARP request for that mapped address comes in on a *different* interface, then you need to manually configure an ARP entry for that network on the ingress interface, specifying its MAC address. Typically, if you specify any interface for the mapped interface, then you use a unique network for the mapped addresses, so this situation would not occur. Configure the ARP table in the ingress interface's **Advanced** settings.

Addresses on a Unique Network

If you need more addresses than are available on the destination (mapped) interface network, you can identify addresses on a different subnet. The upstream router needs a static route for the mapped addresses that points to the FTD device.

Alternatively for routed mode, you can configure a static route on the FTD device for the mapped addresses using any IP address on the destination network as the gateway, and then redistribute the route using your routing protocol. For example, if you use NAT for the inside network (10.1.1.0/24) and use the mapped IP address 209.165.201.5, then you can configure a static route for 209.165.201.5 255.255.255.255 (host address) to the 10.1.1.99 gateway that can be redistributed.

For transparent mode, if the real host is directly-connected, configure the static route on the upstream router to point to the FTD device: specify the bridge group IP address. For remote hosts in transparent mode, in the static route on the upstream router, you can alternatively specify the downstream router IP address.

The Same Address as the Real Address (Identity NAT)

The default behavior for identity NAT has proxy ARP enabled, matching other static NAT rules. You can disable proxy ARP if desired. You can also disable proxy ARP for regular static NAT if desired, in which case you need to be sure to have proper routes on the upstream router.

Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues. For example, if you configure a broad identity NAT rule for “any” IP address, then leaving proxy ARP enabled can cause problems for hosts on the network directly connected to the mapped interface. In this case, when a host on the mapped network wants to communicate with another host on the same network, then the address

in the ARP request matches the NAT rule (which matches “any” address). The FTD device will then proxy ARP for the address, even though the packet is not actually destined for the FTD device. (Note that this problem occurs even if you have a manual NAT rule; although the NAT rule must match both the source and destination addresses, the proxy ARP decision is made only on the “source” address). If the FTD device ARP response is received before the actual host ARP response, then traffic will be mistakenly sent to the FTD device.

Guidelines for NAT

The following topics provide detailed guidelines for implementing NAT.

Firewall Mode Guidelines for NAT

NAT is supported in routed and transparent firewall mode.

However, configuring NAT on bridge group member interfaces (interfaces that are part of a Bridge Group Virtual Interface, or BVI) has the following restrictions:

- When configuring NAT for the members of a bridge group, you specify the member interface. You cannot configure NAT for the bridge group interface (BVI) itself.
- When doing NAT between bridge group member interfaces, you must specify the real and mapped addresses. You cannot specify “any” as the interface.
- You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.
- You cannot translate between IPv4 and IPv6 networks (NAT64/46) when the source and destination interfaces are members of the same bridge group. Static NAT/PAT 44/66, dynamic NAT44/66, and dynamic PAT44 are the only allowed methods; dynamic PAT66 is not supported.



Note You cannot configure NAT for interfaces operating in inline, inline tap, or passive modes.

IPv6 NAT Guidelines

NAT supports IPv6 with the following guidelines and restrictions.

- For standard routed mode interfaces, you can also translate between IPv4 and IPv6.
- You cannot translate between IPv4 and IPv6 for interfaces that are members of the same bridge group. You can translate between two IPv6 or two IPv4 networks only.
- You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group.
- For static NAT, you can specify an IPv6 subnet up to /64. Larger subnets are not supported.
- When using FTP with NAT46, when an IPv4 FTP client connects to an IPv6 FTP server, the client must use either the extended passive mode (EPSV) or extended port mode (EPRT); PASV and PORT commands are not supported with IPv6.

IPv6 NAT Best Practices

You can use NAT to translate between IPv6 networks, and also to translate between IPv4 and IPv6 networks (routed mode only). We recommend the following best practices:

- **NAT66 (IPv6-to-IPv6)**—We recommend using static NAT. Although you can use dynamic NAT or PAT, IPv6 addresses are in such large supply, you do not have to use dynamic NAT. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (manual NAT only).
- **NAT46 (IPv4-to-IPv6)**—We recommend using static NAT. Because the IPv6 address space is so much larger than the IPv4 address space, you can easily accommodate a static translation. If you do not want to allow returning traffic, you can make the static NAT rule unidirectional (manual NAT only). When translating to an IPv6 subnet (/96 or lower), the resulting mapped address is by default an IPv4-embedded IPv6 address, where the 32-bits of the IPv4 address is embedded after the IPv6 prefix. For example, if the IPv6 prefix is a /96 prefix, then the IPv4 address is appended in the last 32-bits of the address. For example, if you map 192.168.1.0/24 to 201b::0/96, then 192.168.1.4 will be mapped to 201b::0.192.168.1.4 (shown with mixed notation). If the prefix is smaller, such as /64, then the IPv4 address is appended after the prefix, and a suffix of 0s is appended after the IPv4 address. You can also optionally translate the addresses net-to-net, where the first IPv4 address maps to the first IPv6 address, the second to the second, and so on.
- **NAT64 (IPv6-to-IPv4)**—You may not have enough IPv4 addresses to accommodate the number of IPv6 addresses. We recommend using a dynamic PAT pool to provide a large number of IPv4 translations.

NAT Support for Inspected Protocols

Some application layer protocols that open secondary connections, or that embedded IP addresses in packets, are inspected to provide the following services:

- **Pinhole creation**—Some application protocols open secondary TCP or UDP connections either on standard or negotiated ports. Inspection opens pinholes for these secondary ports so that you do not need to create access control rules to allow them.
- **NAT rewrite**—Protocols such as FTP embed IP addresses and ports for the secondary connections in packet data as part of the protocol. If there is NAT translation involved for either of the endpoints, the inspection engines rewrite the packet data to reflect the NAT translation of the embedded addresses and ports. The secondary connections would not work without NAT rewrite.
- **Protocol enforcement**—Some inspections enforce some degree of conformance to the RFCs for the inspected protocol.

The following table lists the inspected protocols that apply NAT rewrite and their NAT limitations. Keep these limitations in mind when writing NAT rules that include these protocols. Inspected protocols not listed here do not apply NAT rewrite. These inspections include GTP, HTTP, IMAP, POP, SMTP, SSH, and SSL.



Note NAT rewrite is supported on the listed ports only. For some of these protocols, you can extend inspection to other ports using Network Analysis Policies, but NAT rewrite is not extended to those ports. This includes DCERPC, DNS, FTP, and Sun RPC inspection. If you use these protocols on non-standard ports, do not use NAT on the connections.

Table 2: NAT Supported Application Inspection

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
DCERPC	TCP/135	No NAT64.	Yes
DNS over UDP	UDP/53	No NAT support is available for name resolution through WINS.	No
ESMTP	TCP/25	No NAT64.	No
FTP	TCP/21	(Clustering) No static PAT.	Yes
H.323 H.225 (Call signaling) H.323 RAS	TCP/1720 UDP/1718 For RAS, UDP/1718-1719	(Clustering) No static PAT. No extended PAT. No NAT64.	Yes
ICMP ICMP Error	ICMP (ICMP traffic directed to a device interface is never inspected.)	No limitations.	No
IP Options	RSVP	No NAT64.	No
NetBIOS Name Server over IP	UDP/137, 138 (Source ports)	No extended PAT. No NAT64.	No
RSH	TCP/514	No PAT. No NAT64. (Clustering) No static PAT.	Yes
RTSP	TCP/554 (No handling for HTTP cloaking.)	No extended PAT. No NAT64. (Clustering) No static PAT.	Yes
SIP	TCP/5060 UDP/5060	No extended PAT. No NAT64 or NAT46. (Clustering) No static PAT.	Yes
Skinny (SCCP)	TCP/2000	No extended PAT. No NAT64, NAT46, or NAT66. (Clustering) No static PAT.	Yes
SQL*Net (versions 1, 2)	TCP/1521	No extended PAT. No NAT64. (Clustering) No static PAT.	Yes

Application	Inspected Protocol, Port	NAT Limitations	Pinholes Created
Sun RPC	TCP/111 UDP/111	No extended PAT. No NAT64.	Yes
TFTP	UDP/69	No NAT64. (Clustering) No static PAT. Payload IP addresses are not translated.	Yes
XDMCP	UDP/177	No extended PAT. No NAT64. (Clustering) No static PAT.	Yes

Additional Guidelines for NAT

- (Auto NAT only.) You can only define a single NAT rule for a given object; if you want to configure multiple NAT rules for an object, you need to create multiple objects with different names that specify the same IP address.
- If you define a site-to-site VPN on a device that is behind a device that is applying dynamic PAT, so that UDP ports 500 and 4500 are not the ones actually used, you must initiate the connection from the device that is behind the PAT device. The responder cannot initiate the security association (SA) because it does not know the correct port numbers.
- If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT configuration is used, you can clear the translation table using the **clear xlate** command in the device CLI. However, clearing the translation table disconnects all current connections that use translations. Use the **system support** command to enter the diagnostic CLI, where you have access to the **clear xlate** command.

If you create a new NAT rule that should apply to an existing connection (such as a VPN tunnel), you need to use **clear conn** to end the connection. Then, the attempt to re-establish the connection should hit the NAT rule and the connection should be NAT'ed correctly.



Note If you remove a dynamic NAT or PAT rule, and then add a new rule with mapped addresses that overlap the addresses in the removed rule, then the new rule will not be used until all connections associated with the removed rule time out or are cleared using the **clear xlate** or **clear conn** commands. This safeguard ensures that the same address is not assigned to multiple hosts.

- You cannot use an object group with both IPv4 and IPv6 addresses; the object group must include only one type of address.
- (Manual NAT only.) When using **any** as the source address in a NAT rule, the definition of “any” traffic (IPv4 vs. IPv6) depends on the rule. Before the FTD device performs NAT on a packet, the packet must be IPv6-to-IPv6 or IPv4-to-IPv4; with this prerequisite, the FTD device can determine the value of **any** in a NAT rule. For example, if you configure a rule from “any” to an IPv6 server, and that server was



mapped from an IPv4 address, then **any** means “any IPv6 traffic.” If you configure a rule from “any” to “any,” and you map the source to the interface IPv4 address, then **any** means “any IPv4 traffic” because the mapped interface address implies that the destination is also IPv4.

- You can use the same mapped object or group in multiple NAT rules.
- The mapped IP address pool cannot include:
 - The mapped interface IP address. If you specify “any” interface for the rule, then all interface IP addresses are disallowed. For interface PAT (routed mode only), specify the interface name instead of the interface address.
 - The failover interface IP address.
 - (Transparent mode.) The management IP address.
- Avoid using overlapping addresses in static and dynamic NAT policies. For example, with overlapping addresses, a PPTP connection can fail to get established if the secondary connection for PPTP hits the static instead of dynamic xlate.
- You cannot use overlapping addresses in the source address of a NAT rule and a remote access VPN address pool.
- If you specify a destination interface in a rule, then that interface is used as the egress interface rather than looking up the route in the routing table. However, for identity NAT, you have the option to use a route lookup instead.
- NAT applies to through traffic only. Traffic generated by the system is not subject to NAT.
- Do not name a network object or group pat-pool, using any combination of upper- or lower-case letters.
- You cannot use NAT on the internal payload of Protocol Independent Multicast (PIM) registers.
- (Manual NAT) When writing NAT rules for a dual ISP interface setup (primary and backup interfaces using service level agreements in the routing configuration), do not specify destination criteria in the rule. Ensure the rule for the primary interface comes before the rule for the backup interface. This allows the device to choose the correct NAT destination interface based on the current routing state when the primary ISP is unavailable. If you specify destination objects, the NAT rule will always select the primary interface for the otherwise duplicate rules.
- If you get the ASP drop reason nat-no-xlate-to-pat-pool for traffic that should not match the NAT rules defined for the interface, configure identity NAT rules for the affected traffic so the traffic can pass untranslated.
- If you configure NAT for GRE tunnel endpoints, you must disable keepalives on the endpoints or the tunnel cannot be established. The endpoints send keepalives to the original addresses.

Configure NAT for Threat Defense

Network address translation can be very complex. We recommend that you keep your rules as simple as possible to avoid translation problems and difficult troubleshooting situations. Careful planning before you implement NAT is critical. The following procedure provides the basic approach.

Procedure

- Step 1** Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.
- Step 2** Decide what kinds of rules you need.
- You can create dynamic NAT, dynamic PAT, static NAT, and identity NAT rules. For an overview, see [NAT Types, on page 2](#).
- Step 3** Decide which rules should be implemented as manual or auto NAT.
- For a comparison of these two implementation options, see [Auto NAT and Manual NAT, on page 5](#).
- Step 4** Create the rules as explained in the following sections.
- [Dynamic NAT, on page 15](#)
 - [Dynamic PAT, on page 20](#)
 - [Static NAT, on page 27](#)
 - [Identity NAT, on page 35](#)
- Step 5** Manage the NAT policy and rules.
- You can do the following to manage the policy and its rules.
- To change whether a rule is enabled or disabled, right click the rule and select the desired option from the **State** command. You can temporarily disable a rule without deleting it using these controls.
 - To edit a rule, click **Edit** () for the rule.
 - To delete a rule, click **Delete** () for the rule.
- Step 6** Click **Save**.
- You can now click **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.
-

Dynamic NAT

The following topics explain dynamic NAT and how to configure it.

About Dynamic NAT

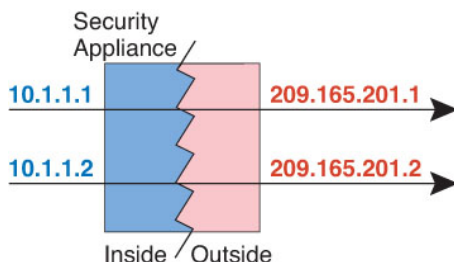
Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The mapped pool typically includes fewer addresses than the real group. When a host you want to translate accesses the destination network, NAT assigns the host an IP address from the mapped pool. The translation is created only when the real host initiates the connection. The translation is in place only for the duration of the connection, and a given user does not keep the same IP address after the translation times out. Users on the destination network, therefore, cannot initiate a reliable connection to a host that uses dynamic NAT, even if the connection is allowed by an access rule.



Note For the duration of the translation, a remote host can initiate a connection to the translated host if an access rule allows it. Because the address is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

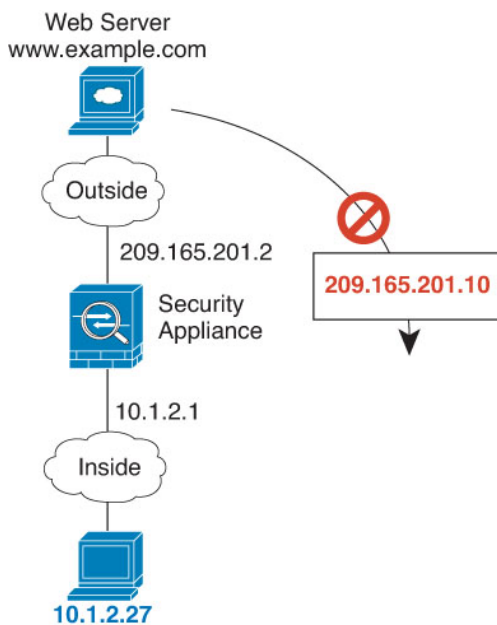
The following figure shows a typical dynamic NAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back.

Figure 4: Dynamic NAT



The following figure shows a remote host attempting to initiate a connection to a mapped address. This address is not currently in the translation table; therefore, the packet is dropped.

Figure 5: Remote Host Attempts to Initiate a Connection to a Mapped Address



Dynamic NAT Disadvantages and Advantages

Dynamic NAT has these disadvantages:

- If the mapped pool has fewer addresses than the real group, you could run out of addresses if the amount of traffic is more than expected.

Use PAT or a PAT fall-back method if this event occurs often because PAT provides over 64,000 translations using ports of a single address.

- You have to use a large number of routable addresses in the mapped pool, and routable addresses may not be available in large quantities.

The advantage of dynamic NAT is that some protocols cannot use PAT. PAT does not work with the following:

- IP protocols that do not have a port to overload, such as GRE version 0.
- Some multimedia applications that have a data stream on one port, the control path on another port, and are not open standard.

Configure Dynamic Auto NAT


Use dynamic auto NAT rules to translate addresses to different IP addresses that are routable on the destination network.

Before you begin

Select **Objects > Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host or subnet. You must select the **Allow Overrides** option.
- **Translated Source**—This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

Procedure

-
- Step 1** Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.
- Step 2** Do one of the following:
- Select **Add NAT Rule > Add Auto NAT** to create a new rule.
 - Click **Edit** () to edit an existing rule.
- The right click menu also has options to cut, copy, paste, insert, and delete rules.
- Step 3** Configure the basic rule options:
- **Type**—Select **Dynamic**.
 - **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.
- Step 4** On **General**, configure the following options:
- **Original Source**—The network object that contains the addresses you are translating.
 - **Translated Source**—The network object or group that contains the mapped addresses.

- Step 5** (Optional.) On **Advanced**, select the desired options:
- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records.
 - **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option.
 - **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- Step 6** Click **Save** to add the rule.
- Step 7** Click **Save** on the NAT page to save your changes.
-

Configure Dynamic Manual NAT

Use dynamic manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Dynamic NAT translates addresses to different IP addresses that are routable on the destination network.

Before you begin


Select **Objects > Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—This can be a network object or group, but it cannot include a subnet.

You can also create network objects for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule.

For dynamic NAT, you can also perform port translation on the destination. In the Object Manager, ensure that there are port objects you can use for the **Original Destination Port** and **Translated Destination Port**. If you specify the source port, it will be ignored.

Procedure

- Step 1** Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.
- Step 2** Do one of the following:
- Select **Add NAT Rule > Add Manual NAT** to create a new rule.
 - Click **Edit** () to edit an existing rule.

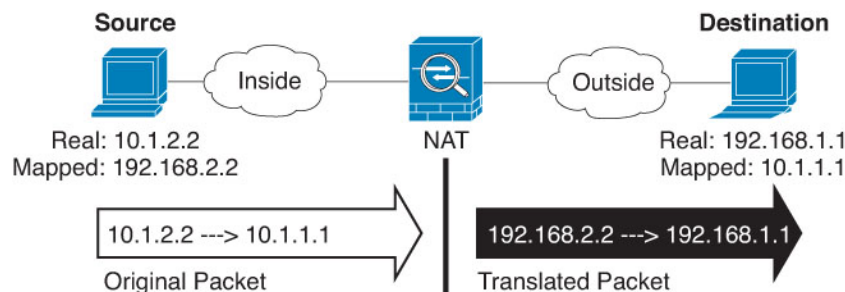
The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **Type**—Select **Dynamic**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.
- **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 4 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 5 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—The network object or group that contains the mapped addresses.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 6 (Optional.) Identify the destination service ports for service translation: **Original Destination Port, Translated Destination Port**.

Dynamic NAT does not support port translation, so leave the **Original Source Port** and **Translated Source Port** fields empty. However, because the destination translation is always static, you can perform port translation for the destination port.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

Step 7 (Optional.) On **Advanced**, select the desired options:

- (For source translation only.) **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records.
- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.

Step 8 Click **Save** to add the rule.

Step 9 Click **Save** on the NAT page to save your changes.

Dynamic PAT

The following topics describe dynamic PAT.

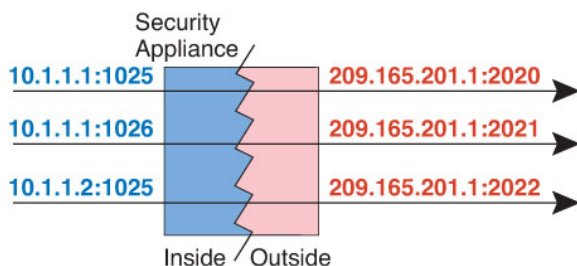
About Dynamic PAT

Dynamic PAT translates multiple real addresses to a single mapped IP address by translating the real address and source port to the mapped address and a unique port.

Each connection requires a separate translation session because the source port differs for each connection. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The following figure shows a typical dynamic PAT scenario. Only real hosts can create a NAT session, and responding traffic is allowed back. The mapped address is the same for each translation, but the port is dynamically assigned.

Figure 6: Dynamic PAT



For the duration of the translation, a remote host on the destination network can initiate a connection to the translated host if an access rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case you can rely on the security of the access rule.

After the connection expires, the port translation also expires.



Note We recommend that you use different PAT pools for each interface. If you use the same pool for multiple interfaces, especially if you use it for "any" interface, the pool can be quickly exhausted, with no ports available for new translations.

Dynamic PAT Disadvantages and Advantages

Dynamic PAT lets you use a single mapped address, thus conserving routable addresses. You can even use the FTD device interface IP address as the PAT address.

You cannot use dynamic PAT for IPv6 (NAT66) when translating between interfaces in the same bridge group.

Dynamic PAT does not work with some multimedia applications that have a data stream that is different from the control path. For more information, see [NAT Support for Inspected Protocols, on page 11](#).

Dynamic PAT might also create a large number of connections appearing to come from a single IP address, and servers might interpret the traffic as a DoS attack. You can configure a PAT pool of addresses and use a round-robin assignment of PAT addresses to mitigate this situation.

PAT Pool Object Guidelines

When creating network objects for a PAT pool, follow these guidelines.

For a PAT pool

- If available, the real source port number is used for the mapped port. However, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 0 to 511, 512 to 1023, and 1024 to 65535. Therefore, ports below 1024 have only a small PAT pool that can be used. If you have a lot of traffic that uses the lower port ranges, you can specify a flat range of ports to be used instead of the three unequal-sized tiers: either 1024 to 65535, or 1 to 65535.
- If you use the same PAT pool object in two separate rules, then be sure to specify the same options for each rule. For example, if one rule specifies extended PAT, then the other rule must also specify extended PAT.
- If a host has an existing connection, then subsequent connections from that host use the same PAT IP address. If no ports are available, this can prevent the connection. Use the round robin option to avoid this problem.
- For best performance, limit the number of IP addresses within a PAT pool to 10,000.

For extended PAT for a PAT pool

- Many application inspections do not support extended PAT.
- If you enable extended PAT for a dynamic PAT rule, then you cannot also use an address in the PAT pool as the PAT address in a separate static NAT with port translation rule. For example, if the PAT pool includes 10.1.1.1, then you cannot create a static NAT-with-port-translation rule using 10.1.1.1 as the PAT address.
- If you use a PAT pool and specify an interface for fallback, you cannot specify extended PAT.

- For VoIP deployments that use ICE or TURN, do not use extended PAT. ICE and TURN rely on the PAT binding to be the same for all destinations.
- Extended PAT increases memory usage on the device.

For round robin for a PAT pool

- If a host has an existing connection, then subsequent connections from that host will use the same PAT IP address if ports are available. However, this “stickiness” does not survive a failover. If the device fails over, then subsequent connections from a host might not use the initial IP address.
- IP address “stickiness” is also impacted if you mix PAT pool/round robin rules with interface PAT rules on the same interface. For any given interface, choose either a PAT pool or interface PAT; do not create competing PAT rules.
- Round robin, especially when combined with extended PAT, can consume a large amount of memory. Because NAT pools are created for every mapped protocol/IP address/port range, round robin results in a large number of concurrent NAT pools, which use memory. Extended PAT results in an even larger number of concurrent NAT pools.

Configure Dynamic Auto PAT

Use dynamic auto PAT rules to translate addresses to unique IP address/port combinations, rather than to multiple IP addresses only. You can translate to a single address (either the destination interface's address or another address), or use a PAT pool of addresses to provide a larger number of possible translations.

Before you begin

Select **Objects > Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host or subnet. You must select the **Allow Overrides** option.
- **Translated Source**—You have the following options to specify the PAT address:
 - **Destination Interface**—To use the destination interface address, you do not need a network object.
 - **Single PAT address**—Create a network object containing a single host.
 - **PAT pool**—Create a network object group that contains more than one host address. You cannot include subnets. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.

Procedure

-
- Step 1** Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.
- Step 2** Do one of the following:
- Select **Add NAT Rule > Add Auto NAT** to create a new rule.

- Click **Edit** (🔧) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **Type**—Select **Dynamic**.
- **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 4 On **General**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—One of the following:
 - (Interface PAT.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Skip the step for configuring a PAT pool.
 - To use a single address other than the destination interface address, select the host network object you created for this purpose. Skip the step for configuring a PAT pool.
 - To use a PAT pool, leave **Translated Source** empty.

Step 5 If you are using a PAT pool, select the **PAT Pool** page and do the following:

- a) Select **Enable PAT pool**.
- b) Select the network object group that contains the addresses for the pool in the **PAT > Address** field.
You can alternatively select **Interface**, which is another way to implement interface PAT.
- c) (Optional) Select the following options as needed:
 - **Use Round Robin Allocation**—To assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
 - **Extended PAT Table**—To use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80. You cannot use this option with interface PAT or interface PAT fallback.
 - **Flat Port Range, Include Reserved Ports**—To use the 1024 to 65535 port range as a single flat range when allocating TCP/UDP ports. When choosing the mapped port number for a translation, PAT uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also check the **Include Reserved Ports** option.

- Step 6** (Optional.) On **Advanced**, select the desired options:
- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option. You cannot select this option if you already configured interface PAT as the translated address or PAT pool.
 - **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- Step 7** Click **Save** to add the rule.
- Step 8** Click **Save** on the NAT page to save your changes.
-

Configure Dynamic Manual PAT

Use dynamic manual PAT rules when auto PAT does not meet your needs. For example, if you want to do different translations based on the destination. Dynamic PAT translates addresses to unique IP address/port combinations, rather than to multiple IP addresses only. You can translate to a single address (either the destination interface's address or another address), or use a PAT pool of addresses to provide a larger number of possible translations.

Before you begin

Select **Objects > Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—You have the following options to specify the PAT address:
 - **Destination Interface**—To use the destination interface address, you do not need a network object.
 - **Single PAT address**—Create a network object containing a single host.
 - **PAT pool**—Create a network object group that contains more than one host address. You cannot include subnets.

You can also create network objects for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule.

For dynamic NAT, you can also perform port translation on the destination. In the Object Manager, ensure that there are port objects you can use for the **Original Destination Port** and **Translated Destination Port**. If you specify the source port, it will be ignored.

Procedure

- Step 1** Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.
- Step 2** Do one of the following:
- Select **Add NAT Rule > Add Manual NAT** to create a new rule.

- Click **Edit** (🔧) to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3

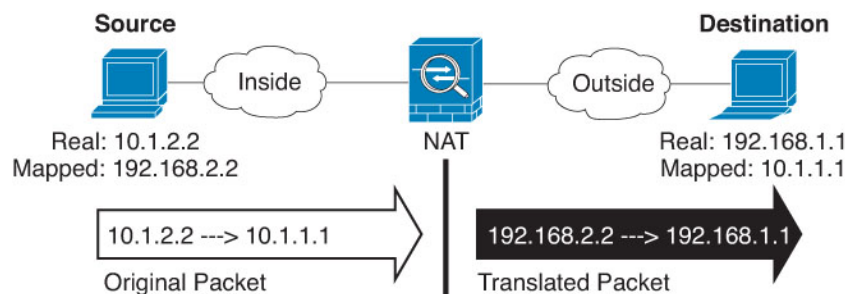
Configure the basic rule options:

- **Type**—Select **Dynamic**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.
- **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 4

Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 5

Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—One of the following:
 - (Interface PAT.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Skip the step for configuring a PAT pool.
 - To use a single address other than the destination interface address, select the host network object you created for this purpose. Skip the step for configuring a PAT pool.

- To use a PAT pool, leave **Translated Source** empty.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 6 (Optional.) Identify the destination service ports for service translation: **Original Destination Port**, **Translated Destination Port**.

Dynamic NAT does not support port translation, so leave the **Original Source Port** and **Translated Source Port** fields empty. However, because the destination translation is always static, you can perform port translation for the destination port.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

Step 7 If you are using a PAT pool, select the **PAT Pool** page and do the following:

- Select **Enable PAT pool**.
- Select the network object group that contains the addresses for the pool in the **PAT > Address** field.

You can alternatively select **Interface**, which is another way to implement interface PAT.

- (Optional) Select the following options as needed:

- **Use Round Robin Allocation**—To assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.
- **Extended PAT Table**—To use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80. You cannot use this option with interface PAT or interface PAT fallback.
- **Flat Port Range, Include Reserved Ports**—To use the 1024 to 65535 port range as a single flat range when allocating TCP/UDP ports. When choosing the mapped port number for a translation, PAT uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also check the **Include Reserved Ports** option.

Step 8 (Optional.) On **Advanced**, select the desired options:

- **Fallthrough to Interface PAT (Destination Interface)**—Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.

Step 9 Click **Save** to add the rule.

Step 10 Click **Save** on the NAT page to save your changes.

Static NAT

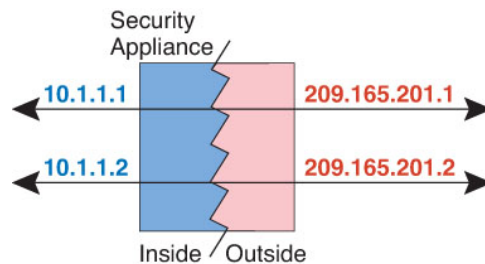
The following topics explain static NAT and how to implement it.

About Static NAT

Static NAT creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if an access rule exists that allows it). With dynamic NAT and PAT, on the other hand, each host uses a different address or port for each subsequent translation, so bidirectional initiation is not supported.

The following figure shows a typical static NAT scenario. The translation is always active so both real and remote hosts can initiate connections.

Figure 7: Static NAT



Note You can disable bidirectionality if desired.

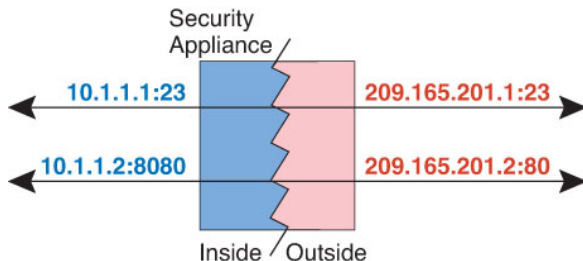
Static NAT with Port Translation

Static NAT with port translation lets you specify a real and mapped protocol and port.

When you specify the port with static NAT, you can choose to map the port and/or the IP address to the same value or to a different value.

The following figure shows a typical static NAT with port translation scenario showing both a port that is mapped to itself and a port that is mapped to a different value; the IP address is mapped to a different value in both cases. The translation is always active so both translated and remote hosts can initiate connections.

Figure 8: Typical Static NAT with Port Translation Scenario



Static NAT-with-port-translation rules limit access to the destination IP address for the specified port only. If you try to access the destination IP address on a different port not covered by a NAT rule, then the connection is blocked. In addition, for manual NAT, traffic that does not match the source IP address of the NAT rule will be dropped if it matches the destination IP address, regardless of the destination port. Therefore, you must add additional rules for all other traffic allowed to the destination IP address. For example, you can configure a static NAT rule for the IP address, without port specification, and place it after the port translation rule.



Note For applications that require application inspection for secondary channels (for example, FTP and VoIP), NAT automatically translates the secondary ports.

Following are some other uses of static NAT with port translation.

Static NAT with Identity Port Translation

You can simplify external access to internal resources. For example, if you have three separate servers that provide services on different ports (such as FTP, HTTP, and SMTP), you can give external users a single IP address to access those services. You can then configure static NAT with identity port translation to map the single external IP address to the correct IP addresses of the real servers based on the port they are trying to access. You do not need to change the port, because the servers are using the standard ones (21, 80, and 25 respectively).

Static NAT with Port Translation for Non-Standard Ports

You can also use static NAT with port translation to translate a well-known port to a non-standard port or vice versa. For example, if inside web servers use port 8080, you can allow outside users to connect to port 80, and then undo translation to the original port 8080. Similarly, to provide extra security, you can tell web users to connect to non-standard port 6785, and then undo translation to port 80.

Static Interface NAT with Port Translation

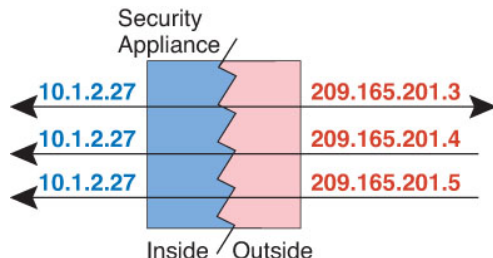
You can configure static NAT to map a real address to an interface address/port combination. For example, if you want to redirect Telnet access for the device's outside interface to an inside host, then you can map the inside host IP address/port 23 to the outside interface address/port 23.

One-to-Many Static NAT

Typically, you configure static NAT with a one-to-one mapping. However, in some cases, you might want to configure a single real address to several mapped addresses (one-to-many). When you configure one-to-many static NAT, when the real host initiates traffic, it always uses the first mapped address. However, for traffic initiated to the host, you can initiate traffic to any of the mapped addresses, and they will be untranslated to the single real address.

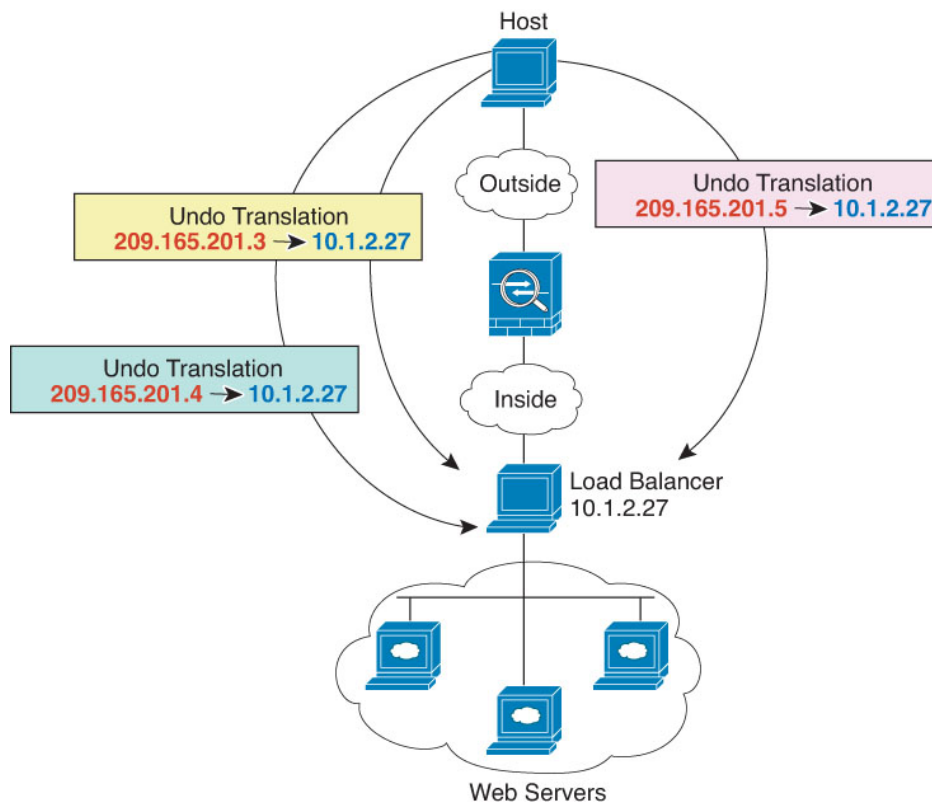
The following figure shows a typical one-to-many static NAT scenario. Because initiation by the real host always uses the first mapped address, the translation of real host IP/first mapped IP is technically the only bidirectional translation.

Figure 9: One-to-Many Static NAT



For example, you have a load balancer at 10.1.2.27. Depending on the URL requested, it redirects traffic to the correct web server.

Figure 10: One-to-Many Static NAT Example



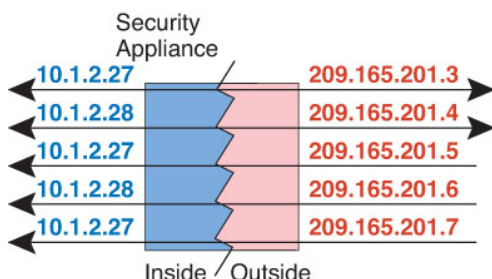
Other Mapping Scenarios (Not Recommended)

NAT has the flexibility to allow any kind of static mapping scenario: one-to-one, one-to-many, but also few-to-many, many-to-few, and many-to-one mappings. We recommend using only one-to-one or one-to-many mappings. These other mapping options might result in unintended consequences.

Functionally, few-to-many is the same as one-to-many; but because the configuration is more complicated and the actual mappings may not be obvious at a glance, we recommend creating a one-to-many configuration for each real address that requires it. For example, for a few-to-many scenario, the few real addresses are mapped to the many mapped addresses in order (A to 1, B to 2, C to 3). When all real addresses are mapped, the next mapped address is mapped to the first real address, and so on until all mapped addresses are mapped (A to 4, B to 5, C to 6). This results in multiple mapped addresses for each real address. Just like a one-to-many configuration, only the first mappings are bidirectional; subsequent mappings allow traffic to be initiated *to* the real host, but all traffic *from* the real host uses only the first mapped address for the source.

The following figure shows a typical few-to-many static NAT scenario.

Figure 11: Few-to-Many Static NAT



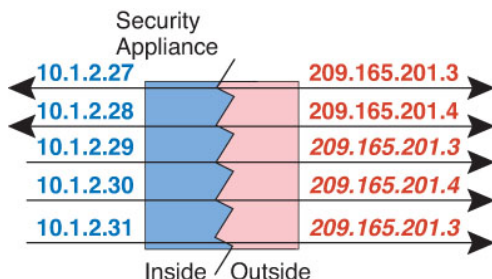
For a many-to-few or many-to-one configuration, where you have more real addresses than mapped addresses, you run out of mapped addresses before you run out of real addresses. Only the mappings between the lowest real IP addresses and the mapped pool result in bidirectional initiation. The remaining higher real addresses can initiate traffic, but traffic cannot be initiated to them (returning traffic for a connection is directed to the correct real address because of the unique 5-tuple (source IP, destination IP, source port, destination port, protocol) for the connection).



Note Many-to-few or many-to-one NAT is not PAT. If two real hosts use the same source port number and go to the same outside server and the same TCP destination port, and both hosts are translated to the same IP address, then both connections will be reset because of an address conflict (the 5-tuple is not unique).

The following figure shows a typical many-to-few static NAT scenario.

Figure 12: Many-to-Few Static NAT



Instead of using a static rule this way, we suggest that you create a one-to-one rule for the traffic that needs bidirectional initiation, and then create a dynamic rule for the rest of your addresses.

Configure Static Auto NAT

Use static auto NAT rules to translate addresses to different IP addresses that are routable on the destination network. You can also do port translation with the static NAT rule.

Before you begin


Select **Objects > Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host or subnet. You must select the **Allow Overrides** option.
- **Translated Source**—You have the following options to specify the translated address:
 - **Destination Interface**—To use the destination interface address, you do not need a network object. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
 - **Address**—Create a network object or group containing hosts or subnets. A group cannot contain both IPv4 and IPv6 addresses; it must contain one type only. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.

Procedure

Step 1 Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.

Step 2 Do one of the following:

- Select **Add NAT Rule > Add Auto NAT** to create a new rule.
- Click **Edit** () to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **Type**—Select **Static**.
- **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 4 On **General**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—One of the following:
 - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.

- (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
- (Optional.) **Original Port, Translated Port**—If you need to translate a TCP or UDP port, select the protocol in **Original Port**, and type the original and translated port numbers. For example, you can translate TCP/80 to 8080 if necessary.

Step 5 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. This option is not available if you are doing port translation.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- **Net to Net Mapping**—For NAT 46, select this option to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this option.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

Step 6 Click **Save** to add the rule.

Step 7 Click **Save** on the NAT page to save your changes.

Configure Static Manual NAT

Use static manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Static NAT translates addresses to different IP addresses that are routable on the destination network. You can also do port translation with the static NAT rule.

Before you begin

Select **Objects > Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:


- **Original Source**—This can be a network object or group, and it can contain a host or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—You have the following options to specify the translated address:

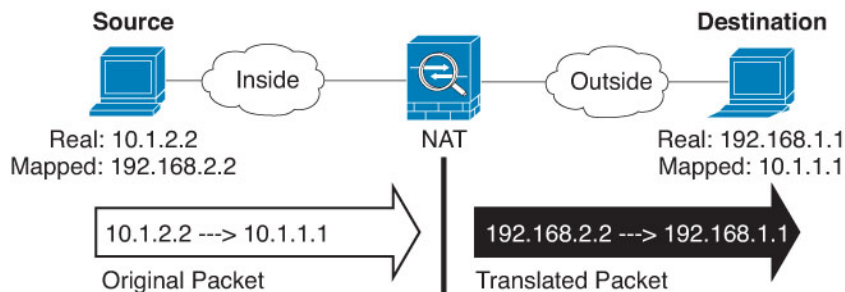
- **Destination Interface**—To use the destination interface address, you do not need a network object. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
- **Address**—Create a network object or group containing hosts or subnets. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.

You can also create network objects for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule. If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses and specify the interface in the rule.

You can also perform port translation on the source, destination, or both. In the Object Manager, ensure that there are port objects you can use for the original and translated ports.

Procedure

- Step 1** Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.
- Step 2** Do one of the following:
- Select **Add NAT Rule > Add Manual NAT** to create a new rule.
 - Click **Edit** () to edit an existing rule.
- The right click menu also has options to cut, copy, paste, insert, and delete rules.
- Step 3** Configure the basic rule options:
- **Type**—Select **Static**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.
 - **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
 - **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.
 - **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.
- Step 4** Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.
- See the following figure for an example of the original packet vs. the translated packet.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 5 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—One of the following:
 - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
 - (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 6 (Optional.) Identify the source or destination service ports for service translation.

If you are configuring static NAT with port translation, you can translate ports for the source, destination, or both. For example, you can translate between TCP/80 and TCP/8080.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

- **Original Source Port, Translated Source Port**—Defines a port translation for the source address.
- **Original Destination Port, Translated Destination Port**—Defines a port translation for the destination address.

Step 7 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. This option is not available if you are doing port translation.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- **Net to Net Mapping**—For NAT 46, select this option to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this option.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.
- **Unidirectional**—Select this option to prevent the destination addresses from initiating traffic to the source addresses. The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.

Step 8 Click **Save** to add the rule.

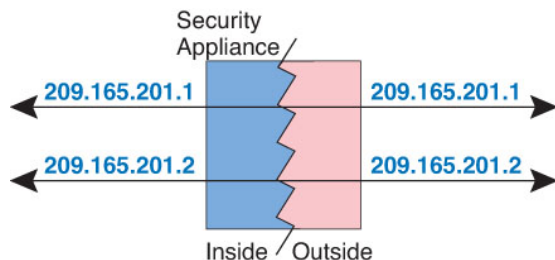
Step 9 Click **Save** on the NAT page to save your changes.

Identity NAT

You might have a NAT configuration in which you need to translate an IP address to itself. For example, if you create a broad rule that applies NAT to every network, but want to exclude one network from NAT, you can create a static NAT rule to translate an address to itself.

The following figure shows a typical identity NAT scenario.

Figure 13: Identity NAT



The following topics explain how to configure identity NAT.

Configure Identity Auto NAT

Use static identity auto NAT rules to prevent the translation of an address. That is, to translate the address to itself.

Before you begin


Select **Objects > Object Management** and create the network objects or groups needed in the rule. Alternatively, you can create the objects while defining the NAT rule. The objects must meet the following requirements:

- **Original Source**—This must be a network object (not a group), and it can be a host or subnet. You must select the **Allow Overrides** option.
- **Translated Source**—A network object or group with the exact same contents as the original source object. You can use the same object.

Procedure

Step 1 Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.

Step 2 Do one of the following:

- Select **Add NAT Rule > Add Auto NAT** to create a new rule.
- Click **Edit** () to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

Step 3 Configure the basic rule options:

- **Type**—Select **Static**.
- **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 4 On **General**, configure the following options:

- **Original Source**—The network object that contains the addresses you are translating.
- **Translated Source**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Do not configure the **Original Port** and **Translated Port** options for identity NAT.

Step 5 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Do not configure this option for identity NAT.
- **IPv6**—Do not configure this option for identity NAT.
- **Net to Net Mapping**—Do not configure this option for identity NAT.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to

have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

- **Perform Route Lookup for Destination Interface**— If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Step 6 Click **Save** to add the rule.

Step 7 Click **Save** on the NAT page to save your changes.

Configure Identity Manual NAT

Use static identity manual NAT rules when auto NAT does not meet your needs. For example, if you want to do different translations based on the destination. Use static identity NAT rules to prevent the translation of an address. That is, to translate the address to itself.

Before you begin

Select **Objects > Object Management** and create the network objects or groups needed in the rule. Groups cannot contain both IPv4 and IPv6 addresses; they must contain one type only. Alternatively, you can create the objects while defining the NAT rule. The objects must also meet the following requirements:

- **Original Source**—This can be a network object or group, and it can contain a host or subnet. If you want to translate all original source traffic, you can skip this step and specify **Any** in the rule.
- **Translated Source**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.


You can also create network objects for the **Original Destination** and **Translated Destination** if you are configuring a static translation for those addresses in the rule. If you want to configure destination static interface NAT with port translation only, you can skip adding an object for the destination mapped addresses and specify the interface in the rule.

You can also perform port translation on the source, destination, or both. In the Object Manager, ensure that there are port objects you can use for the original and translated ports. You can use the same object for identity NAT.

Procedure

Step 1 Choose **Devices > Device Management**, and edit the Firepower Threat Defense device. Select **NAT**.

Step 2 Do one of the following:

- Select **Add NAT Rule > Add Manual NAT** to create a new rule.
- Click **Edit** () to edit an existing rule.

The right click menu also has options to cut, copy, paste, insert, and delete rules.

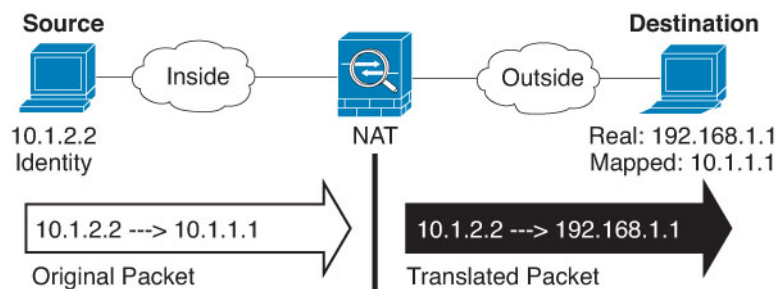
Step 3 Configure the basic rule options:

- **Type**—Select **Static**. This setting only applies to the source address. If you define a translation for the destination address, the translation is always static.

- **Enable**—Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page.
- **Insert**—Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.
- **Source Interface, Destination Interface**—(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Step 4 Identify the original packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear in the original packet.

See the following figure for an example of the original packet vs. the translated packet where you perform identity NAT on the inside host but translate the outside host.



- **Original Source**—The network object or group that contains the addresses you are translating.
- **Original Destination**—(Optional.) The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Step 5 Identify the translated packet addresses, either IPv4 or IPv6; namely, the packet addresses as they appear on the destination interface network. You can translate between IPv4 and IPv6 if desired.

- **Translated Source**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.
- **Translated Destination**—(Optional.) The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Step 6 (Optional.) Identify the source or destination service ports for service translation.

If you are configuring static NAT with port translation, you can translate ports for the source, destination, or both. For example, you can translate between TCP/80 and TCP/8080.

NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

- **Original Source Port, Translated Source Port**—Defines a port translation for the source address.
- **Original Destination Port, Translated Destination Port**—Defines a port translation for the destination address.

Step 7 (Optional.) On **Advanced**, select the desired options:

- **Translate DNS replies that match this rule**—Do not configure this option for identity NAT.
- **IPv6**—Whether to use the IPv6 address of the destination interface for interface PAT.
- **Do not proxy ARP on Destination Interface**—Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.
- **Perform Route Lookup for Destination Interface**— If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.
- **Unidirectional**—Select this option to prevent the destination addresses from initiating traffic to the source addresses. The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.

Step 8 Click **Save** to add the rule.

Step 9 Click **Save** on the NAT page to save your changes.

NAT Rule Properties for Firepower Threat Defense

Use Network Address Translation (NAT) rules to translate IP addresses to other IP addresses. You would typically use NAT rules to convert private addresses to publically routable addresses. The translation can be from one address to another, or you can use Port Address Translation (PAT) to translate many addresses to one or a few addresses, using port numbers to distinguish among the source addresses.

NAT rules include the following basic properties. The properties are the same for auto NAT and manual NAT rules except where indicated.

Type

Whether the translation rule is **Dynamic** or **Static**. Dynamic translation automatically chooses the mapped address from a pool of addresses, or an address/port combination when implementing PAT. Use static translation if you want to precisely define the mapped address/port.

Source Interface, Destination Interface

(Required for bridge group member interfaces.) The interfaces where this NAT rule applies. **Source** is the real interface, the one through which the traffic enters the device. **Destination** is the mapped interface, the one through which traffic exits the device. By default, the rule applies to all interfaces (**Any**) except for bridge group member interfaces.

Enable (Manual NAT only.)

Whether you want the rule to be active. You can later activate or deactivate the rule using the right-click menu on the rules page. You cannot disable auto NAT rules.

Insert (Manual NAT only.)

Where you want to add the rule. You can insert it in a category (before or after auto NAT rules), or above or below the rule number you specify.

Description (Optional. Manual NAT only.)

A description of the purpose of the rule.

The following topics describe the tabs for the NAT rules properties.

General Properties for Auto NAT

Use the options on **General** to define the source addresses and the mapped translated addresses. The following properties apply to auto NAT only.

Original Source (Always required.)

The network object that contains the addresses you are translating. This must be a network object (not a group), and it can be a host or subnet. You must select the **Allow Overrides** option in the object, but do not define an override.

You cannot create auto NAT rules for the system-defined any-ipv4 or any-ipv6 objects.

Translated Source (Usually required.)

The mapped addresses, the ones to which you are translating. What you select here depends on the type of translation rule you are defining.

- **Dynamic NAT**—The network object or group that contains the mapped addresses. This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
- **Dynamic PAT**—One of the following:
 - (Interface PAT.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Do not configure a PAT pool.
 - To use a single address other than the destination interface address, select the host network object you created for this purpose. Do not configure a PAT pool.
 - To use a PAT pool, leave **Translated Source** empty. Select the PAT pool object on **PAT Pool**.
- **Static NAT**—One of the following:
 - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. The object or group can contain hosts or subnets. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
 - (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on the **Advanced** tab. This configures

static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.

- **Identity NAT**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Original Port, Translated Port (Static NAT only.)

If you need to translate a TCP or UDP port, select the protocol in **Original Port**, and type the original and translated port numbers. For example, you can translate TCP/80 to 8080 if necessary. Do not configure these options for identity NAT.

General Properties for Manual NAT

Use the options on **General** to define the source addresses and the mapped translated addresses. The following properties apply to manual NAT only. All are optional except as indicated.

Original Source (Always required.)

The network object or group that contains the addresses you are translating. This can be a network object or group, and it can contain a host or subnet. If you want to translate all original source traffic, you can specify **Any** in the rule.

Translated Source (Usually required.)

The mapped addresses, the ones to which you are translating. What you select here depends on the type of translation rule you are defining.

- **Dynamic NAT**—The network object or group that contains the mapped addresses. This can be a network object or group, but it cannot include a subnet. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
- **Dynamic PAT**—One of the following:
 - (Interface PAT.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on **Advanced**. Do not configure a PAT pool.
 - To use a single address other than the destination interface address, select the host network object you created for this purpose. Do not configure a PAT pool.
 - To use a PAT pool, leave **Translated Source** empty. Select the PAT pool object on **PAT Pool**.
- **Static NAT**—One of the following:
 - To use a set group of addresses, select **Address** and the network object or group that contains the mapped addresses. The object or group can contain hosts or subnets. Typically, you configure the same number of mapped addresses as real addresses for a one-to-one mapping. You can, however, have a mismatched number of addresses.
 - (Static interface NAT with port translation.) To use the address of the destination interface, select **Interface**. You must also select a specific destination interface. To use the IPv6 address of the interface, you must also select the **IPv6** option on the **Advanced** tab. This configures static interface NAT with port translation: the source address/port is translated to the interface's address and the same port number.

- **Identity NAT**—The same object as the original source. Optionally, you can select a different object that has the exact same contents.

Original Destination

The network object that contains the addresses of the destinations. If you leave this blank, the source address translation applies regardless of destination. If you do specify the destination address, you can configure a static translation for that address or just use identity NAT for it.

You can select **Interface** to base the original destination on the source interface (which cannot be Any). If you select this option, you must also select a translated destination object. To implement a static interface NAT with port translation for the destination addresses, select this option and also select the appropriate port objects for the destination ports.

Translated Destination

The network object or group that contains the destination addresses used in the translated packet. If you selected an object for **Original Destination**, you can set up identity NAT (that is, no translation) by selecting the same object.

Original Source Port, Translated Source Port, Original Destination Port, Translated Destination Port

The port objects that define the source and destination services for the original and translated packets. You can translate the ports, or select the same object to make the rule sensitive to the service without translating the ports. Keep the following rules in mind when configuring services:

- (Dynamic NAT or PAT.) You cannot do translation on the **Original Source Port** and **Translated Source Port**. You can do translation on the destination port only.
- NAT only supports TCP or UDP. When translating a port, be sure the protocols in the real and mapped service objects are identical (both TCP or both UDP). For identity NAT, you can use the same service object for both the real and mapped ports.

PAT Pool NAT Properties

When you configure dynamic NAT, you can define a pool of addresses to use for Port Address Translation using the properties on the **PAT Pool** tab.

Enable PAT Pool

Select this option to configure a pool of addresses for PAT.

PAT

The addresses to use for the PAT pool, one of the following:

- **Address**—The network object group that contains the host addresses for the PAT pool. You cannot include subnets. The group cannot contain both IPv4 and IPv6 addresses; it must contain one type only.
- **Interface**—Indicates that you want to use the destination interface as the PAT address. For this option, you must select a specific **Destination Interface**; you cannot use **Any** as the destination interface. This is another way to implement interface PAT.

Round Robin

To assign addresses/ports in a round-robin fashion. By default without round robin, all ports for a PAT address will be allocated before the next PAT address is used. The round-robin method assigns one

address/port from each PAT address in the pool before returning to use the first address again, and then the second address, and so on.

Extended PAT Table

To use extended PAT. Extended PAT uses 65535 ports per *service*, as opposed to per IP address, by including the destination address and port in the translation information. Normally, the destination port and address are not considered when creating PAT translations, so you are limited to 65535 ports per PAT address. For example, with extended PAT, you can create a translation of 10.1.1.1:1027 when going to 192.168.1.7:23 as well as a translation of 10.1.1.1:1027 when going to 192.168.1.7:80. You cannot use this option with interface PAT or interface PAT fallback.

Flat Port Range; Include Reserved Ports

To use the 1024 to 65535 port range as a single flat range when allocating TCP/UDP ports. When choosing the mapped port number for a translation, PAT uses the real source port number if it is available. However, without this option, if the real port is *not* available, by default the mapped ports are chosen from the same range of ports as the real port number: 1 to 511, 512 to 1023, and 1024 to 65535. To avoid running out of ports at the low ranges, configure this setting. To use the entire range of 1 to 65535, also check the **Include Reserved Ports** option.

Advanced NAT Properties

When you configure NAT, you can configure properties that provide specialized services in the **Advanced** options. All of these properties are optional: configure them only if you need the service.

Translate DNS replies that match this rule

Whether to translate the IP address in DNS replies. For DNS replies traversing from a mapped interface to a real interface, the Address (the IPv4 A or IPv6 AAAA) record is rewritten from the mapped value to the real value. Conversely, for DNS replies traversing from a real interface to a mapped interface, the record is rewritten from the real value to the mapped value. This option is used in specific circumstances, and is sometimes needed for NAT64/46 translation, where the rewrite also converts between A and AAAA records. This option is not available if you are doing port translation in a static NAT rule.

Fallthrough to Interface PAT (Destination Interface) (Dynamic NAT only.)

Whether to use the IP address of the destination interface as a backup method when the other mapped addresses are already allocated (interface PAT fallback). This option is available only if you select a destination interface that is not a member of a bridge group. To use the IPv6 address of the interface, also check the **IPv6** option. You cannot select this option if you already configured interface PAT as the translated address. You also cannot select the option if you configure a PAT pool.

IPv6

Whether to use the IPv6 address of the destination interface for interface PAT.

Net to Net Mapping (Static NAT only.)

For NAT 46, select this option to translate the first IPv4 address to the first IPv6 address, the second to the second, and so on. Without this option, the IPv4-embedded method is used. For a one-to-one translation, you must use this option.

Do not proxy ARP on Destination Interface (Static NAT only.)

Disables proxy ARP for incoming packets to the mapped IP addresses. If you use addresses on the same network as the mapped interface, the system uses proxy ARP to answer any ARP requests for the mapped addresses, thus intercepting traffic destined for a mapped address. This solution simplifies routing because

the device does not have to be the gateway for any additional networks. You can disable proxy ARP if desired, in which case you need to be sure to have proper routes on the upstream router. Normally for identity NAT, proxy ARP is not required, and in some cases can cause connectivity issues.

Perform Route Lookup for Destination Interface (Static Identity NAT only. Routed mode only.)

If you select source and destination interfaces when selecting the same object for original and translated source address, you can select this option to have the system determine the destination interface based on the routing table rather than using the destination interface configured in the NAT rule.

Unidirectional (Manual NAT only, static NAT only.)

Select this option to prevent the destination addresses from initiating traffic to the source addresses. The unidirectional option is mainly useful for testing purposes and might not work with all protocols. For example, SIP requires protocol inspection to translate SIP headers using NAT, but this will not occur if you make the translation unidirectional.

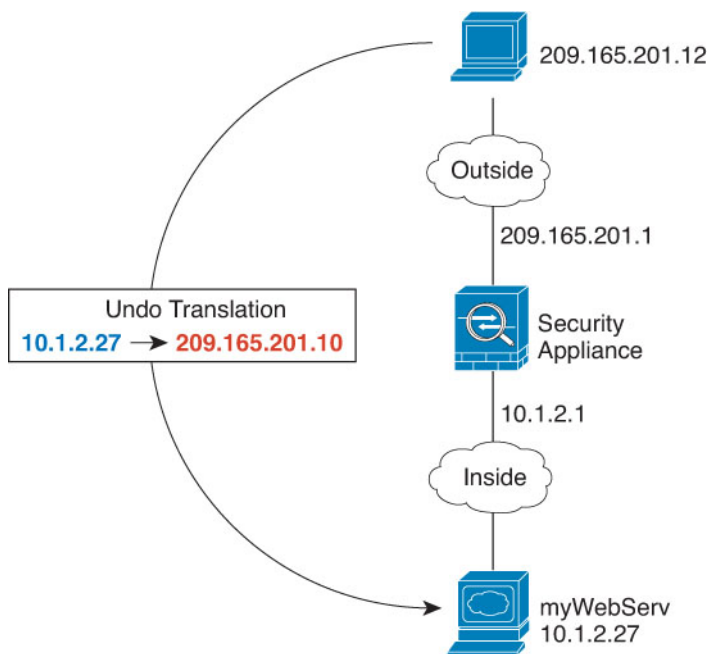
Examples for NAT

The following topics provide examples for configuring NAT on Threat Defense devices.

Providing Access to an Inside Web Server (Static Auto NAT)

The following example performs static NAT for an inside web server. The real address is on a private network, so a public address is required. Static NAT is necessary so hosts can initiate traffic to the web server at a fixed address.

Figure 14: Static NAT for an Inside Web Server



Procedure

Step 1 Create the network objects that define the server's private and public host addresses.

- Choose **Objects > Object Management**.
- Select **Network** from the table of contents and click **Add Network > Add Object**.
- Define the web server's private address.

Name the network object (for example, WebServerPrivate) and enter the real host IP address, 10.1.2.27. Select the **Allow Overrides** option, but do not define an override.

Edit Network Objects

Name:

Description:

Network:

Allow Overrides:

Override (0)

- Click **Save**.
- Click **Add Network > Add Object** and define the public address.

Name the network object (for example, WebServerPublic) and enter the host address 209.165.201.10.

New Network Objects

Name:

Description:

Network:

Allow Overrides:

Override (0)

- Click **Save**.

Step 2 Configure static NAT for the object.

- Select **Devices > Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

- Click **Add NAT Rule > Add Auto NAT**.
- Configure the following properties:

- **Type** = Static.
- **Source Interface** = inside.

- **Destination Interface** = outside.
- **Original Source** = WebServerPrivate network object.
- **Translated Source > Address**= WebServerPublic network object.

Add NAT Rule ? x

Type: **Static** Enable Translated By: barbosa-ftpd-5512

Source Interface: **inside** Destination Interface: **outside**

General PAT Pool Advance

Original Packet

Original Source*: **WebServerPrivate**

Original Port: **TCP**

Translated Packet

Translated Source: **Address** **WebServerPublic**

Translated Port:

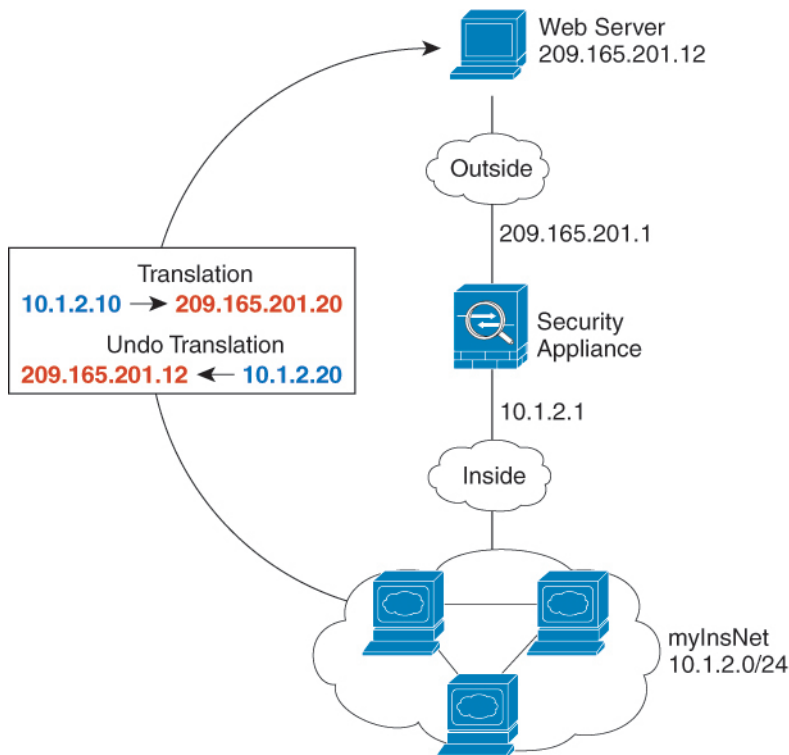
d) Click **Save**.

Step 3 Click **Save** on the NAT rule page.

Dynamic Auto NAT for Inside Hosts and Static NAT for an Outside Web Server

The following example configures dynamic NAT for inside users on a private network when they access the outside. Also, when inside users connect to an outside web server, that web server address is translated to an address that appears to be on the inside network.

Figure 15: Dynamic NAT for Inside, Static NAT for Outside Web Server

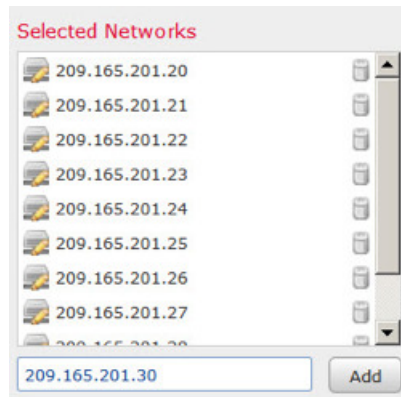


248773

Procedure

- Step 1** Create a network object group for the dynamic NAT pool to which you want to translate the inside addresses.
- Choose **Objects > Object Management**.
 - Select **Network** from the table of contents and click **Add Network > Add Group**.
 - Define the dynamic NAT pool.

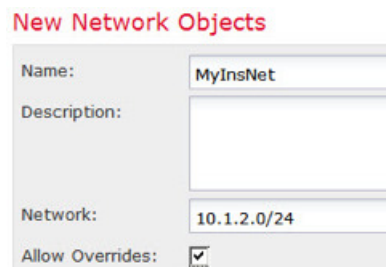
Name the network object (for example, myNATpool). Enter each of the 11 host addresses between 209.165.201.20 and 209.165.201.30 separately in the “inline” edit box below the Selected Networks list and click **Add**.



- Click **Save**.

- Step 2** Create a network object for the inside network.

- Click **Add Network > Add Object**.
- Name the network object (for example, MyInsNet) and enter the network address 10.1.2.0/24. Select the **Allow Overrides** option, but do not define an override.



- Click **Save**.

- Step 3** Create a network object for the outside web server.

- Click **Add Network > Add Object**.
- Name the network object (for example, MyWebServer) and enter the host address 209.165.201.12. Select the **Allow Overrides** option, but do not define an override.

New Network Objects

Name:	myWebServer
Description:	
Network:	209.165.201.12
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 4 Create a network object for the translated web server address.

- a) Click **Add Network > Add Object**.
- b) Name the network object (for example, TransWebServer) and enter the host address 10.1.2.20.

New Network Objects

Name:	TransWebServer
Description:	
Network:	10.1.2.20
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 5 Configure dynamic NAT for the inside network using the dynamic NAT pool object.

- a) Select **Devices > Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

- b) Click **Add NAT Rule > Add Auto NAT**.
- c) Configure the following properties:
 - **Type** = Dynamic.
 - **Source Interface** = inside.
 - **Destination Interface** = outside.
 - **Original Source** = myInsNet network object.
 - **Translated Source > Address** = myNATpool network group.

Add NAT Rule

Type: Enable Translated By:

Source Interface: Destination Interface:

General PAT Pool Advance

Original Packet

Original Source:*

Original Port:

Translated Packet

Translated Source:

Translated Port:

d) Click **Save**.

Step 6 Configure static NAT for the web server.

a) Click **Add NAT Rule** > **Add Auto NAT**.

b) Configure the following properties:

- **Type** = Static.
- **Source Interface** = outside.
- **Destination Interface** = inside.
- **Original Source** = myWebServer network object.
- **Translated Source** > **Address**= TransWebServer network object.

Add NAT Rule

Type: Enable Translated By:

Source Interface: Destination Interface:

General PAT Pool Advance

Original Packet

Original Source:*

Original Port:

Translated Packet

Translated Source:

Translated Port:

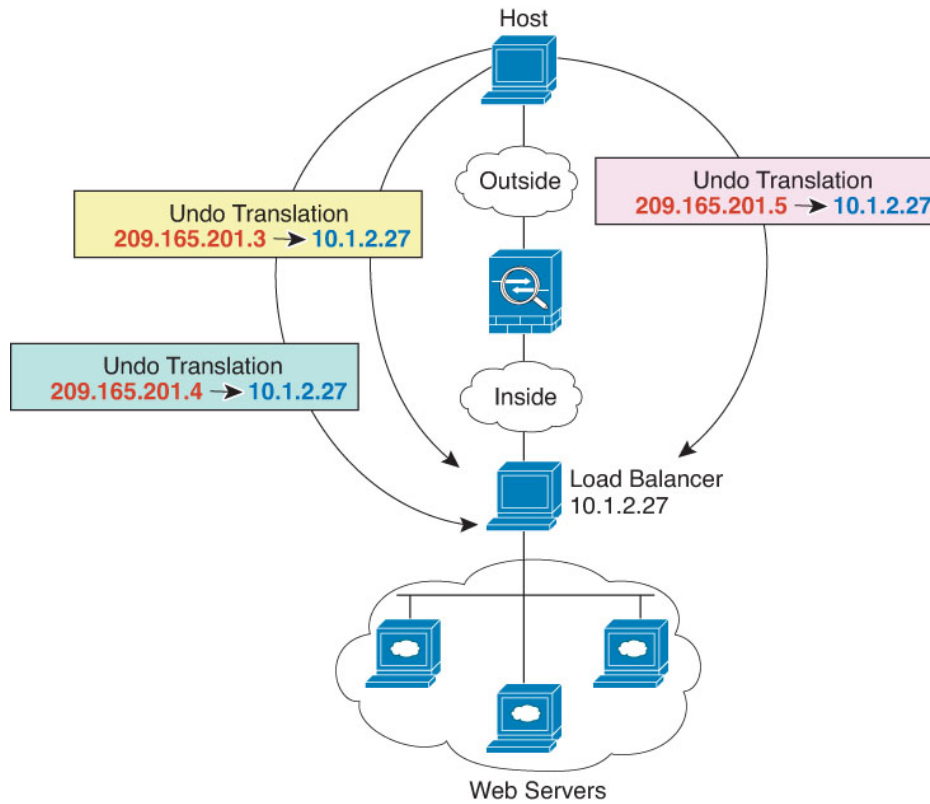
c) Click **Save**.

Step 7 Click **Save** on the NAT rule page.

Inside Load Balancer with Multiple Mapped Addresses (Static Auto NAT, One-to-Many)

The following example shows an inside load balancer that is translated to multiple IP addresses. When an outside host accesses one of the mapped IP addresses, it is untranslated to the single load balancer address. Depending on the URL requested, it redirects traffic to the correct web server.

Figure 16: Static NAT with One-to-Many for an Inside Load Balancer

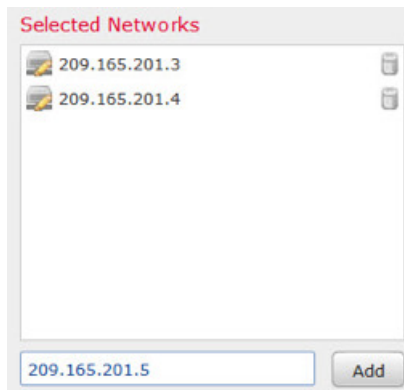


Procedure

Step 1 Create a network object group for the addresses to which you want to map the load balancer.

- Choose **Objects > Object Management**.
- Select **Network** from the table of contents and click **Add Network > Add Group**.
- Define the addresses.

Name the network object (for example, myPublicIPs). Enter each of the 3 host addresses, 209.165.201.3, 209.165.201.4, and 209.165.201.5, separately in the “inline” edit box below the Selected Networks list and click **Add**.

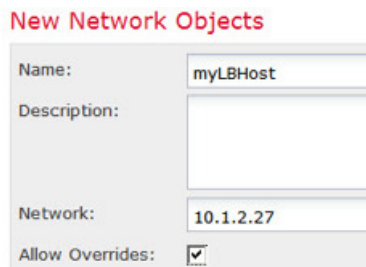


d) Click **Save**.

Step 2

Create a network object for the load balancer.

- Click **Add Network > Add Object**.
- Name the network object (for example, myLBHost), enter the host address 10.1.2.27. Select the **Allow Overrides** option, but do not define an override.



c) Click **Save**.

Step 3

Configure static NAT for the load balancer.

- Select **Devices > Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

- Click **Add NAT Rule > Add Auto NAT**.
- Configure the following properties:
 - **Type** = Static.
 - **Source Interface** = inside.
 - **Destination Interface** = outside.
 - **Original Source** = myLBHost network object.
 - **Translated Source > Address** = myPublicIPs network group.

Add NAT Rule

Type:	Static	<input checked="" type="checkbox"/> Enable	Translated By:	barbosa-fptd-5512
Source Interface:	inside		Destination Interface:	outside
General PAT Pool Advance				
Original Packet		Translated Packet		
Original Source:*	myLBHost	Translated Source:	Address	myPublicIPs
Original Port:	TCP	Translated Port:		

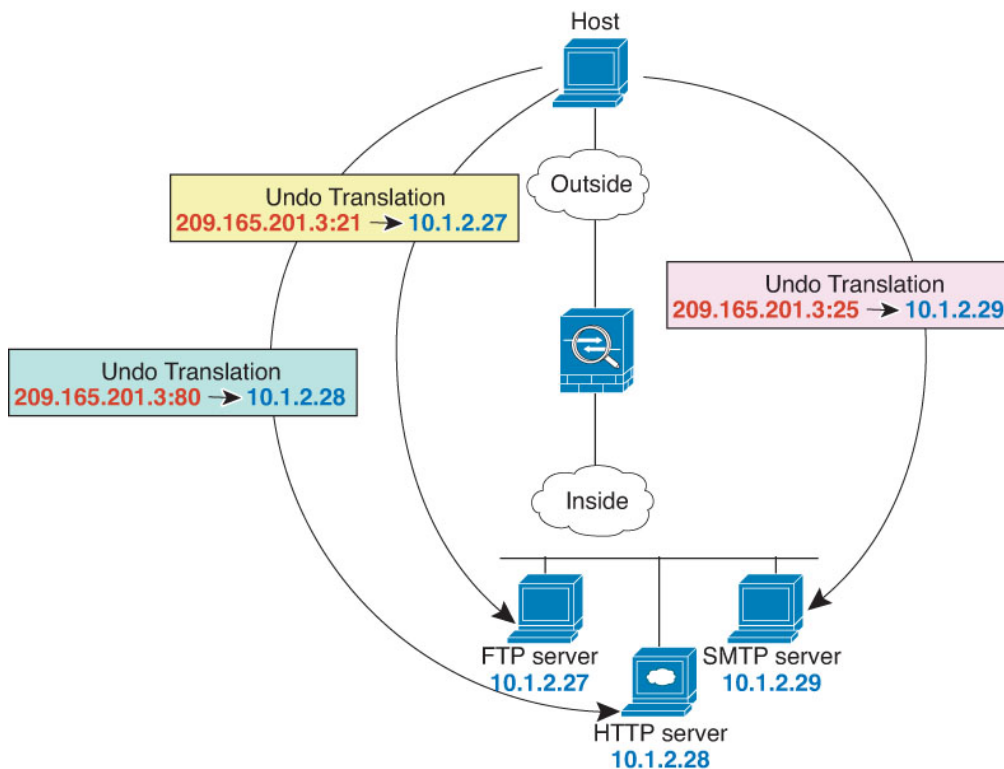
d) Click **Save**.

Step 4 Click **Save** on the NAT rule page.

Single Address for FTP, HTTP, and SMTP (Static Auto NAT-with-Port-Translation)

The following static NAT-with-port-translation example provides a single address for remote users to access FTP, HTTP, and SMTP. These servers are actually different devices on the real network, but for each server, you can specify static NAT-with-port-translation rules that use the same mapped IP address, but different ports.

Figure 17: Static NAT-with-Port-Translation



Procedure

- Step 1** Create a network object for the FTP server.
- Choose **Objects > Object Management**.
 - Select **Network** from the table of contents and click **Add Network > Add Object**.
 - Name the network object (for example, FTPserver), and enter the real IP address for the FTP server, 10.1.2.27. Select the **Allow Overrides** option, but do not define an override.

New Network Objects

Name:	FTPserver
Description:	
Network:	10.1.2.27
Allow Overrides:	<input checked="" type="checkbox"/>

- Click **Save**.

- Step 2** Create a network object for the HTTP server.
- Click **Add Network > Add Object**.
 - Name the network object (for example, HTTPserver), enter the host address 10.1.2.28. Select the **Allow Overrides** option, but do not define an override.

New Network Objects

Name:	HTTPserver
Description:	
Network:	10.1.2.28
Allow Overrides:	<input checked="" type="checkbox"/>

- Click **Save**.

- Step 3** Create a network object for the SMTP server.
- Click **Add Network > Add Object**.
 - Name the network object (for example, SMTPserver), enter the host address 10.1.2.29. Select the **Allow Overrides** option, but do not define an override.

Edit Network Objects

Name:	SMTPserver
Description:	
Network:	10.1.2.29
Allow Overrides:	<input checked="" type="checkbox"/>

- Click **Save**.

Step 4 Create a network object for the public IP address used for the three servers.

- a) Click **Add Network > Add Object**.
- b) Name the network object (for example, ServerPublicIP) and enter the host address 209.165.201.3.

New Network Objects

Name:	ServerPublicIP
Description:	
Network:	209.165.201.3
Allow Overrides:	<input checked="" type="checkbox"/>

- c) Click **Save**.

Step 5 Configure static NAT with port translation for the FTP server, mapping the FTP port to itself.

- a) Select **Devices > Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

- b) Click **Add NAT Rule > Add Auto NAT**.
- c) Configure the following properties:
 - **Type** = Static.
 - **Source Interface** = inside.
 - **Destination Interface** = outside.
 - **Original Source** = FTPserver network object.
 - **Translated Source > Address**= ServerPublicIP network object.
 - **Original Port > TCP** = 21.
 - **Translated Port** = 21.

Add NAT Rule

Type:	Static	<input checked="" type="checkbox"/> Enable	Translated By:	barbosa-fptd-5512
Source Interface:	inside		Destination Interface:	outside

General PAT Pool Advance

Original Packet	Translated Packet
Original Source:*	Translated Source:
FTPserver	Address ServerPublicIP
Original Port:	Translated Port:
TCP 21	21

- d) Click **Save**.

Step 6 Configure static NAT with port translation for the HTTP server, mapping the HTTP port to itself.

- a) Click **Add NAT Rule > Add Auto NAT**.
- b) Configure the following properties:
 - **Type** = Static.

- **Source Interface** = inside.
- **Destination Interface** = outside.
- **Original Source** = HTTPserver network object.
- **Translated Source > Address**= ServerPublicIP network object.
- **Original Port > TCP** = 80.
- **Translated Port** = 80.

Add NAT Rule

Type: Enable Translated By:

Source Interface: Destination Interface:

General PAT Pool Advance

Original Packet

Original Source:*

Original Port:

Translated Packet

Translated Source:

Translated Port:

c) Click **Save**.

Step 7 Configure static NAT with port translation for the SMTP server, mapping the SMTP port to itself.

- Click **Add NAT Rule > Add Auto NAT**.
- Configure the following properties:
 - **Type** = Static.
 - **Source Interface** = inside.
 - **Destination Interface** = outside.
 - **Original Source** = SMTPserver network object.
 - **Translated Source > Address**= ServerPublicIP network object.
 - **Original Port > TCP** = 25.
 - **Translated Port** = 25.

Add NAT Rule

Type: Enable Translated By:

Source Interface: Destination Interface:

General PAT Pool Advance

Original Packet

Original Source:*

Original Port:

Translated Packet

Translated Source:

Translated Port:

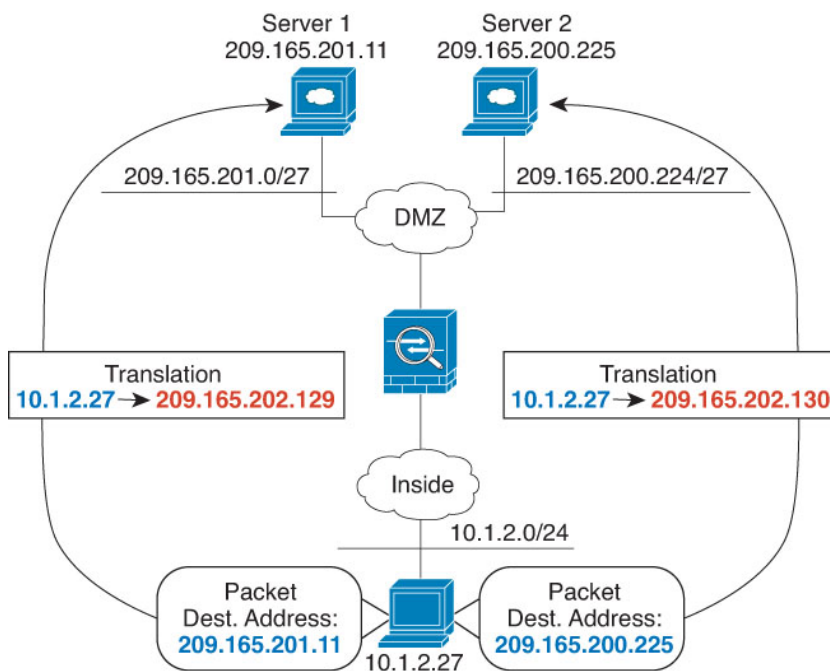
c) Click **Save**.

Step 8 Click **Save** on the NAT rule page.

Different Translation Depending on the Destination (Dynamic Manual PAT)

The following figure shows a host on the 10.1.2.0/24 network accessing two different servers. When the host accesses the server at 209.165.201.11, the real address is translated to 209.165.202.129:port. When the host accesses the server at 209.165.200.225, the real address is translated to 209.165.202.130:port.

Figure 18: Manual NAT with Different Destination Addresses



Procedure

- Step 1** Create a network object for the inside network.
- Choose **Objects > Object Management**.
 - Select **Network** from the table of contents and click **Add Network > Add Object**.
 - Name the network object (for example, myInsideNetwork), and enter the real network address, 10.1.2.0/24.

New Network Objects

Name:	myInsideNetwork
Description:	
Network:	10.1.2.0/24
Allow Overrides:	<input checked="" type="checkbox"/>

d) Click **Save**.

Step 2 Create a network object for the DMZ network 1.

- a) Click **Add Network > Add Object**.
- b) Name the network object (for example, DMZnetwork1) and enter the network address 209.165.201.0/27 (subnet mask of 255.255.255.224).

New Network Objects

Name:	DMZnetwork1
Description:	
Network:	209.165.201.0/27
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 3 Create a network object for the PAT address for DMZ network 1.

- a) Click **Add Network > Add Object**.
- b) Name the network object (for example, PATaddress1) and enter the host address 209.165.202.129.

New Network Objects

Name:	PATaddress1
Description:	
Network:	209.165.202.129
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 4 Create a network object for the DMZ network 2.

- a) Click **Add Network > Add Object**.
- b) Name the network object (for example, DMZnetwork2) and enter the network address 209.165.200.224/27 (subnet mask of 255.255.255.224).

New Network Objects

Name:	DMZnetwork2
Description:	
Network:	209.165.200.224/27
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 5 Create a network object for the PAT address for DMZ network 2.

- a) Click **Add Network > Add Object**.
- b) Name the network object (for example, PATaddress2) and enter the host address 209.165.202.130.

New Network Objects

Name:	PATaddress2
Description:	
Network:	209.165.202.130
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 6

Configure dynamic manual PAT for DMZ network 1.

a) Select **Devices > Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

b) Click **Add NAT Rule > Add Manual NAT**.

c) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source > Address** = PATaddress1 network object.
- **Original Destination > Address** = DMZnetwork1 network object.
- **Translated Destination** = DMZnetwork1 network object.

Note Because you do not want to translate the destination address, you need to configure identity NAT for it by specifying the same address for the original and translated destination addresses. Leave all of the port fields blank.

Add NAT Rule

Type:	Dynamic	<input checked="" type="checkbox"/> Enable	Insert:	In Category	NAT Rules Before																					
Source Interface:	inside		Destination Interface:	dmz																						
Description:																										
<table border="1"> <tr> <td>General</td> <td>PAT Pool</td> <td>Advance</td> </tr> <tr> <td colspan="3">Original Packet</td> <td colspan="3">Translated Packet</td> </tr> <tr> <td>Original Source:*</td> <td>myInsideNetwork</td> <td></td> <td>Translated Source:</td> <td>Address</td> <td>PATaddress1</td> </tr> <tr> <td>Original Destination:</td> <td>Address</td> <td>DMZnetwork1</td> <td>Translated Destination:</td> <td colspan="2">DMZnetwork1</td> </tr> </table>						General	PAT Pool	Advance	Original Packet			Translated Packet			Original Source:*	myInsideNetwork		Translated Source:	Address	PATaddress1	Original Destination:	Address	DMZnetwork1	Translated Destination:	DMZnetwork1	
General	PAT Pool	Advance																								
Original Packet			Translated Packet																							
Original Source:*	myInsideNetwork		Translated Source:	Address	PATaddress1																					
Original Destination:	Address	DMZnetwork1	Translated Destination:	DMZnetwork1																						

d) Click **Save**.

Step 7

Configure dynamic manual PAT for DMZ network 2.

a) Click **Add NAT Rule > Add Manual NAT**.

b) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source > Address** = PATaddress2 network object.
- **Original Destination > Address** = DMZnetwork2 network object.
- **Translated Destination** = DMZnetwork2 network object.

Add NAT Rule

Type:	Dynamic	<input checked="" type="checkbox"/> Enable	Insert:	In Category	NAT Rules Before
Source Interface:	inside		Destination Interface:	dmz	
Description:					
<div style="display: flex; border-bottom: 1px solid #ccc;"> <div style="border-right: 1px solid #ccc; padding: 2px 5px;">General</div> <div style="padding: 2px 5px;">PAT Pool</div> <div style="padding: 2px 5px;">Advance</div> </div>					
Original Packet			Translated Packet		
Original Source:*	myInsideNetwork		Translated Source:	Address	PATaddress2
Original Destination:	Address	DMZnetwork2	Translated Destination:	DMZnetwork2	

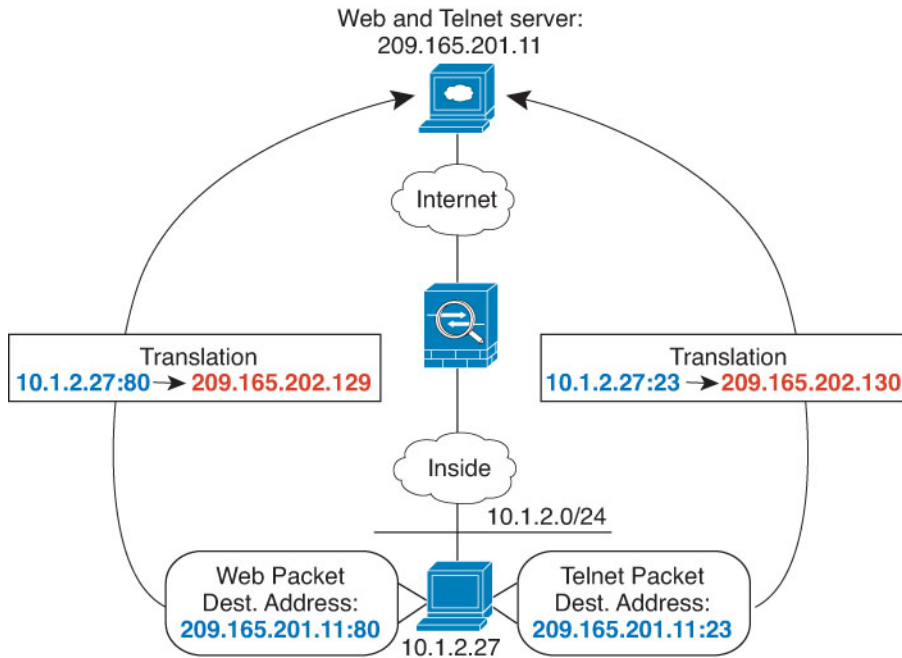
c) Click **Save**.

Step 8 Click **Save** on the NAT rule page.

Different Translation Depending on the Destination Address and Port (Dynamic Manual PAT)

The following figure shows the use of source and destination ports. The host on the 10.1.2.0/24 network accesses a single host for both web services and Telnet services. When the host accesses the server for Telnet services, the real address is translated to 209.165.202.129:port. When the host accesses the same server for web services, the real address is translated to 209.165.202.130:port.

Figure 19: Manual NAT with Different Destination Ports



Procedure

Step 1

Create a network object for the inside network.

- Choose **Objects > Object Management**.
- Select **Network** from the table of contents and click **Add Network > Add Object**.
- Name the network object (for example, myInsideNetwork) and enter the real network address, 10.1.2.0/24.

New Network Objects

Name:	myInsideNetwork
Description:	
Network:	10.1.2.0/24
Allow Overrides:	<input checked="" type="checkbox"/>

- Click **Save**.

Step 2

Create a network object for the Telnet/Web server.

- Click **Add Network > Add Object**.
- Name the network object (for example, TelnetWebServer) and enter the host address 209.165.201.11.

New Network Objects

Name:	TelnetWebServer
Description:	
Network:	209.165.201.11
Allow Overrides:	<input checked="" type="checkbox"/>

New Network Object

Name
TelnetWebServer

Description

Network
 Host Range Network FQDN
209.165.201.11

Allow Overrides

c) Click **Save**.

Step 3 Create a network object for the PAT address when using Telnet.

- Click **Add Network > Add Object**.
- Name the network object (for example, PATAddress1) and enter the host address 209.165.202.129.

New Network Objects

Name:	PATAddress1
Description:	
Network:	209.165.202.129
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 4 Create a network object for the PAT address when using HTTP.

- Click **Add Network > Add Object**.
- Name the network object (for example, PATAddress2) and enter the host address 209.165.202.130.

New Network Objects

Name:	PATAddress2
Description:	
Network:	209.165.202.130
Allow Overrides:	<input checked="" type="checkbox"/>

c) Click **Save**.

Step 5 Configure dynamic manual PAT for Telnet access.

- a) Select **Devices > Device Management** and edit the Threat Defense device on which you are defining the rule. Select **NAT**.

Ensure that you are currently in the same leaf domain that includes the device, if you are using domains.

- b) Click **Add NAT Rule > Add Manual NAT**.

- c) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.
- **Translated Source > Address**= PATaddress1 network object.
- **Original Destination > Address** = TelnetWebServer network object.
- **Translated Destination** = TelnetWebServer network object.
- **Original Destination Port** = TELNET port object (system-defined).
- **Translated Destination Port** = TELNET port object (system-defined).

Note Because you do not want to translate the destination address or port, you need to configure identity NAT for them by specifying the same address for the original and translated destination addresses, and the same port for the original and translated port.

Add NAT Rule

Type:	Dynamic	<input checked="" type="checkbox"/> Enable	Insert:	In Category	NAT Rules Before
Source Interface:	inside		Destination Interface:	dmz	
Description:					
<div style="display: flex; border-bottom: 1px solid #ccc;"> <div style="border-right: 1px solid #ccc; padding: 2px 5px;">General</div> <div style="padding: 2px 5px;">PAT Pool</div> <div style="padding: 2px 5px;">Advance</div> </div>					
Original Packet			Translated Packet		
Original Source:*	myInsideNetwork		Translated Source:	Address	PATaddress1
Original Destination:	Address	TelnetWebServer	Translated Destination:	TelnetWebServer	
Original Source Port:			Translated Source Port:		
Original Destination Port:	TELNET		Translated Destination Port:	TELNET	

- d) Click **Save**.

Step 6 Configure dynamic manual PAT for web access.

- a) Click **Add NAT Rule > Add Manual NAT**.

- b) Configure the following properties:

- **Type** = Dynamic.
- **Source Interface** = inside.
- **Destination Interface** = dmz.
- **Original Source** = myInsideNetwork network object.

- **Translated Source > Address**= PATAddress2 network object.
- **Original Destination > Address** = TelnetWebServer network object.
- **Translated Destination** = TelnetWebServer network object.
- **Original Destination Port** = HTTP port object (system-defined).
- **Translated Destination Port** = HTTP port object (system-defined).

Add NAT Rule

Type: Enable Insert: NAT Rules Before

Source Interface: Destination Interface:

Description:

General PAT Pool Advance

Original Packet

Original Source:*

Original Destination:

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source:

Translated Destination:

Translated Source Port:

Translated Destination Port:

c) Click **Save**.

Step 7 Click **Save** on the NAT rule page.

History for FTD NAT

Feature	Version	Details
Network Address Translation (NAT) for Firepower Threat Defense.	6.0.1	<p>The NAT policy for Firepower Threat Defense was added.</p> <p>New/modified screens: Threat Defense was added as a type of NAT policy to the Devices > NAT page.</p> <p>Supported platforms: Firepower Threat Defense</p>

